MASTER'S THESIS

De invloed van opleiding op Information Security Awareness

van de Mortel, K.

Award date:
2021

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain.
• You may freely distribute the URL identifying the publication in the public portal.

Take down policy
If you believe that this document breaches copyright please contact us at:

pure-support@ou.nl

providing details and we will investigate your claim.

Downloaded from https://research.ou.nl/ on date: 06. May. 2023

Open Universiteit
www.ou.nl

De invloed van opleiding op Information Security Awareness

The influence of education on Information Security Awareness

Opleiding:	Open Universiteit, faculteit Bètawetenschappen
	Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty Science
	Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT
	IM9806 Afstudeeropdracht Business Process Management and IT
Student:	Koen van de Mortel
Identiteitsnummer:	
Datum:	02-04-2021
Afstudeerbegeleider:	Prof. dr. Lex Bijlsma
Examinator:	Dr. Lloyd Rutledge
Derde beoordelaar:	Niet van toepassing
Versie nummer:	1.0
Status:	<definitief>

Abstract

Een hoog Information Security Awareness (ISA) van medewerkers is van groot belang voor organisaties om ongewenst gedrag in de omgang met data te voorkomen en daarmee Information Security risico's te verlagen. Factoren die ISA beïnvloeden kunnen gebruikt worden in educatieve maatregelen. Het doel van dit onderzoek is om meer duidelijkheid te krijgen in de invloed van opleidingsniveau op ISA van medewerkers, zodat educatie mogelijk kan worden afgestemd op het opleidingsniveau. In een online enquête op basis van de HAIS-Q methode zijn gegevens verzameld over het opleidingsniveau en de ISA van alle computergebruikers van een profit organisatie. De resultaten geven aan dat er geen positieve correlatie vastgesteld kan worden tussen opleidingsniveau en ISA. Ook is er geen verschil in kennis, houding of gedrag tussen de verschillende opleidingsniveaus. Een IT-opleiding leidt wel tot een hogere ISA en een IT-opleiding leidt ook tot betere kennis, een betere houding en beter gedrag. Organisaties wordt aanbevolen om een security-training te geven aan werknemers en bedrijven wordt aangeraden een Information Security Policy te hebben en uit te dragen. Verder wetenschappelijk onderzoek naar het verband tussen opleidingsniveau en ISA, bij meerdere en of verschillende bedrijven, wordt aanbevolen omdat de onderzoeksresultaten specifiek kunnen zijn voor de case organisatie.

Sleutelbegrippen

Information Security Awareness (ISA); The Human Aspects of Information Security Questionnaire (HAIS-Q); Information security (InfoSec); Beschikbaarheid, integriteit en vertrouwelijkheid (BIV), Information security policy (ISP).

Samenvatting

Door de groeiende hoeveelheid data binnen bedrijven en het gebruik van internet, thuiswerkers, webshops en de omvang van netwerken is Information Security van groot belang. Ongewenst gedrag ten aanzien van het gebruik van de data door medewerkers kan de Information Security in gevaar brengen. Bedrijven proberen, naast het doorvoeren van technische maatregelen, het gedrag van medewerkers te beïnvloeden door organisatorische en educatieve maatregelen te treffen. Daarvoor is het nodig om te weten welke factoren op dit gedrag van invloed zijn, zodat deze gebruikt kunnen worden in de aanpak om Information Security risico's te verkleinen. In de wetenschappelijke literatuur wordt opleidingsniveau als mogelijke factor genoemd die van invloed is op ISA. Het huidige onderzoek heeft opleidingsniveau als mogelijke factor verder onderzocht. De uitkomst geeft een beeld van de relatie tussen opleidingsniveau en ISA van medewerkers, specifiek in een profit organisatie. Organisaties kunnen deze kennis gebruiken bij de inzet van hun educatieve maatregelen om ISA te verhogen, door educatieve maatregelen af te stemmen op het opleidingsniveau van de medewerker.

Dit leidt tot de volgende probleemstelling: Organisaties zoeken al jaren naar manieren om de ISA van hun medewerkers te verhogen. Door onderzoek zijn inmiddels diverse factoren bekend die van invloed zijn op ISA. Organisaties kunnen deze factoren gebruiken voor de invulling van organisatorische en educatieve maatregelen, om de ISA van hun medewerkers te vergroten en daarmee Infosec risico's te verlagen. Uit onderzoek wordt voor alsnog niet duidelijk of opleidingsniveau één van de factoren is, die van invloed is op ISA.

Doel van het onderzoek is, om de vraag te beantwoorden of er een verband is tussen opleidingsniveau en ISA op de onderdelen kennis, houding en gedrag voor non-technical users in een profit organisatie.

Na een literatuuronderzoek zijn de bevindingen die daaruit naar voren kwamen omgezet in hypothesen die vervolgens getoetst zijn in een praktijk situatie. De belangrijkste hypothese is dat er een verband is tussen opleidingsniveau en ISA. De tweede hypothese is dat opleidingsniveau van invloed is op de kennis, houding en gedrag in het kader van ISA. De laatste hypothese is dat een IT-opleiding van invloed is op ISA. Deze hypothesen zijn getoetst in een empirisch onderzoek dat is uitgevoerd als case study bij een profit organisatie. Werknemers van de case organisatie hebben deelgenomen aan een online enquête gebaseerd op de HAIS-Q methode waarmee hun ISA is gemeten. De antwoorden van de respondenten zijn geanalyseerd en hebben geleid tot de volgende resultaten:

- Er kan geen positieve correlatie vastgesteld worden tussen opleidingsniveau en ISA en ook niet tussen opleidingsniveau en kennis, houding of gedrag.
- Geen enkel opleidingsniveau heeft een significant hogere ISA. Er is ook geen enkel opleidingsniveau wat een significant hogere kennis, betere houding of beter gedrag heeft.
- een IT-opleiding leidt tot een hogere ISA.

Deze resultaten leiden tot de volgende conclusies. De hypothese dat er een verband is tussen opleidingsniveau en ISA wordt verworpen. De hypothese dat opleidingsniveau van invloed is op de kennis, houding en gedrag in het kader van ISA wordt ook verworpen. De hypothese dat een IT-opleiding van invloed is op ISA wordt aangenomen. Samengevat kan gezegd worden dat medewerkers met een hogere opleiding de Information Security regels niet beter of slechter kennen dan mensen met een lagere opleiding. Ook met betrekking tot houding en gedrag is er geen verschil

vast te stellen tussen medewerkers met een hogere of lagere opleiding. Een IT-opleiding leidt tot een hogere ISA en een IT-opleiding leidt ook tot betere kennis, een betere houding en beter gedrag.

Op basis van de conclusies wordt het organisaties aanbevolen om een security-training te geven aan werknemers om het kennisniveau van Information Security op een hoger peil te krijgen. Daarnaast wordt bedrijven aangeraden een Information Security Policy te hebben en uit te dragen. Tenslotte wordt aanbevolen om hetzelfde onderzoek nogmaals uit te voeren bij het bedrijf om over tijd vast te stellen of eventueel genomen educatieve maatregelen effect hebben gehad.

Er dient verder wetenschappelijk onderzoek gedaan te worden naar het verband tussen opleidingsniveau en ISA omdat de onderzoeksresultaten specifiek kunnen zijn voor de case organisatie. Door het onderzoek uit te voeren bij meerdere bedrijven kan meer data verzameld en vergeleken worden. Hierdoor kunnen verschillen of juist overeenkomsten tussen bedrijven en sectoren worden onderzocht. Een andere aanbeveling is om hetzelfde onderzoek na verloop van tijd te herhalen, waarbij het verschil in de gemiddelde scores per opleiding op de diverse aspecten van de HAIS-Q vragenlijst dan direct wordt meegenomen. Tenslotte wordt aanbevolen om te onderzoeken of juist recenter afgestuurde IT'ers verantwoordelijk zijn voor de geconstateerde hogere ISA.

Summary

Due to the growing amount of data within companies and the use of internet, home workers, web shops and the size of networks, Information Security is of great importance. Undesirable behaviour regarding the use of data by employees can endanger Information Security. Companies try, in addition to implementing technical measures, to influence the behaviour of employees by taking organisational and educational measures. It is therefore necessary to know which factors influence this behaviour, so that these can be used in the approach to reduce Information Security risks. In the scientific literature, level of education is mentioned as a possible factor that influences ISA. The current research has further investigated the level of education as a possible factor. The results provide insight in the relationship between educational level and ISA of employees, specifically in a profit organisation. Organisations can use this knowledge when using their educational measures to increase ISA, by matching educational measures to the education level of the employee.

This leads to the following problem statement: For years, organisations have been looking for ways to increase the ISA of their employees. Through research, various factors that influence ISA are now known. Organisations can use these factors to implement organisational and educational measures in order to increase their employees' ISA and thereby reduce Infosec risks. It is still not clear from previous research whether educational level is one of the factors that influence ISA.

The aim of the study is to answer the question of whether there is a link between educational level and ISA in the components of knowledge, attitude and behaviour for non-technical users in a profit organisation.

After a literature study, the findings were converted into hypotheses which were then tested in a practical situation. The main hypothesis is that there is a link between education level and ISA. The second hypothesis is that educational level influences knowledge, attitude and behaviour in the context of ISA. The final hypothesis is that IT education influences ISA. These hypotheses were tested in an empirical study that was carried out as a case study at a profit organisation. Employees of the case organisation participated in an online questionnaire based on the HAIS-Q method used to measure their ISA. The respondents' answers were analysed and led to the following results:

- No positive correlation can be established between education level and ISA, nor between education level and knowledge, attitude or behaviour.

- No educational level has a significantly higher ISA. There is also no education level that has a significantly higher knowledge, attitude or behaviour.

- An IT education leads to a higher ISA.

These results lead to the following conclusions. The hypothesis that there is a relationship between education level and ISA is rejected. The hypothesis that level of education influences knowledge, attitude and behaviour in the context of ISA is also rejected. The hypothesis that IT education influences ISA is accepted. In summary, it can be said that employees with a higher education do know the Information Security rules better neither better nor worse than people with a lower education. Also with regard to attitude and behaviour, no difference can be established between employees with a higher or lower education. An IT education leads to a higher ISA and an IT education also leads to better knowledge, a better attitude and better behaviour.

Based on the conclusions, it is recommended that organisations give security training to employees in order to raise the knowledge level of Information Security to a higher level. In addition, it is

recommended that companies have and propagate an Information Security Policy. Finally, it is recommended that the same research be carried out again at the company in order to determine in time whether any educational measures taken have had an effect.

Further scientific research into the relationship between educational level and ISA should be carried out because the research results may be specific to the case organisation. By conducting the research at several companies, more data can be collected and compared. This way, differences or similarities between companies and sectors can be investigated. Another recommendation is to repeat the same survey over time, whereby the difference in average scores per study programme for the various aspects of the HAIS-Q questionnaire are then also taken into account. Finally, it is recommended to investigate whether more recently graduated IT professionals are responsible for the higher ISA.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

Deze thesis is geschreven in het kader van het afstuderen voor de Masteropleiding Business Process Management & IT aan de Open Universiteit. Het onderwerp van het onderzoek is Security management. De afstudeeropdrachten op dit terrein komen neer op het doorlichten van een organisatie of technologie op beveiligingsaspecten, gebruik makend van daarvoor in de literatuur beschikbare modellen en instrumenten, alsmede het formuleren van managementadviezen ter verbetering. Tegelijkertijd ontstaat daarbij het inzicht hoe de bestaande instrumenten kunnen worden uitgebreid en verbeterd.

Gestart wordt met de gebiedsverkenning, waarna een probleemstelling wordt gedefinieerd. Dan volgt een beschrijving van het doel van het onderzoek met de onderzoeksvragen. Hoofdstuk 1 eindigt met de wetenschappelijke en maatschappelijke relevantie van dit onderzoek. Ten slotte volgt een leeswijzer voor de rest van het rapport waarin in hoofdlijnen de uitvoering van het onderzoek wordt beschreven.

1.2. Gebiedsverkenning

Binnen Security Management zijn beschikbaarheid, integriteit en vertrouwelijkheid van informatie sleutelbegrippen. Information Security (Infosec) heeft de laatste jaren een grote ontwikkeling doorgemaakt door o.a. het gebruik van internet, thuiswerkers, webshops, de omvang van netwerken en het gebruik van een steeds groter wordende hoeveelheid data door bedrijven. Hoe gaan bedrijven om met Infosec en hoe brengen zij informatie over op werknemers. Immers kunnen Infosec “failures” grote financiële gevolgen hebben. Daarvoor haalt McCormac, Zwaans, et al. (2017) cijfers aan uit Coopers (2013). Hierin staat dat hun bevindingen suggereren dat 34% van de security incidenten ontstaan door gedrag van werknemers, daarbij een gemiddeld verlies van $ 2,5 miljoen dollar veroorzakend. Ter bevordering van information security worden door bedrijven technische, organisatorische en educatieve maatregelen genomen. Technische maatregelen, zoals hardware- en softwaresecuritymechanismen, worden breed ingezet om informatiesystemen te beschermen tegen aanvallen. Deze systemen zijn echter nog steeds zeer kwetsbaar tegenover bedreigingen door ongewenst gedrag van gebruikers, gedrag dat nauw verbonden is met hun information security awareness ofwel ISA (Öğütçü, Testik, & Chouseinoglou, 2016). McIlwraith (2016) zegt over Information security: “Research suggests that between 60-75% of all information security incidents are the result of a lack of knowledge and/or understanding amongst an organization's own staff.” Kennis en begrip van information security onder personeel is dus van groot belang voor organisaties.

Educatieve maatregelen moeten zorgen voor een goed ISA van het personeel. ISA kan daarbij worden verdeeld in drie deelgebieden:

- Kennis van het beleid en de procedures die gevolgd moeten worden
- Begrip waarom men zich hier aan dient te houden
- Het feitelijke gedrag ofwel eigen handelen van medewerkers m.b.t. Information security.

Door een of meer van deze drie onderdelen te verbeteren, kan ISA verbeterd worden (McCormac, Zwaans, et al., 2017).

Er is veel onderzoek gedaan naar wat de ISA van werknemers bepaalt of beïnvloed, om zodoende organisatorische en educatieve maatregelen op een dusdanige manier in te kunnen vullen dat het grootste effect wordt bereikt. Met als doel dat werknemers het gewenste gedrag gaan vertonen,

gedrag in het belang van Infosec. Tsohou and Holtkamp (2018) hebben bijvoorbeeld onderzocht welke competenties van gebruikers geassocieerd worden met compliance ten opzichte van Infosec beleid. McCormac, Zwaans, et al. (2017) hebben in hun onderzoek ontdekt dat leeftijd, geslacht en sommige persoonlijke eigenschappen ISA beïnvloeden. Verder stellen zij dat "Factors such as education and InfoSec training could also have an impact on ISA." Kritzinger and Smith (2008) spreken van verschillen in ISA voor professionals versus low-level users en verschillende IT authority levels. Volgens Öğütçü et al. (2016) is er een correlatie tussen opleiding en ISA. Verderop in deze paragraaf kom ik hier op terug.

Maar hoe gedragen medewerkers zich feitelijk ten aanzien van Infosec en waarop is dit gebaseerd? In het onderzoek van Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) wordt gezegd dat er een significante correlatie bestaat tussen kennis en gedrag m.b.t. Infosec regels. Dit veronderstelt dat je van mensen met meer kennis, verantwoordelijker gedrag mag verwachten m.b.t. Infosec onderwerpen. Kritzinger and Smith (2008) spreken in hun rapport naast de technische-, over de "non-technical information security issues." Binnen dit gebied ligt de focus op de verschillende effecten die mensen kunnen hebben op de beveiliging en bescherming van informatie en informatiesystemen. Deze menselijke invloeden kunnen geclassificeerd worden als bewust of onbewust en daarnaast kunnen ze ontstaan van buiten de organisatie of van binnenuit. Kritzinger and Smith (2008) gaan er bijvoorbeeld vanuit dat medewerkers op professional level de benodigde kennis en ervaring hebben voor het omgaan met technical information security issues, opgedaan door opleiding of cursussen: "These issues are mostly confined to the technical departments and employees with proper information security knowledge and work experience. Their knowledge is usually obtained through formal qualifications, such as tertiary degrees/diplomas or industry-related information security courses." Bij medewerkers op non-technical level wordt echter helemaal niet gesproken over opleiding.

Parsons et al. (2014) zeggen: "employers can be relatively confident that improving their employees' knowledge of policy and procedures will have a positive impact on both attitude towards those policies and procedures and employee behaviour. However, our results also indicate that generic courses that do not attempt to influence attitude and instead simply lecture on knowledge of policy and procedure will be far less effective. Instead, training should be contextualised and should use case studies to improve both knowledge of what is expected and also understanding of why this is important ." Het vergroten van de kennis van het Infosec beleid en procedures lijkt dus de belangrijkste stap te zijn naar een groter ISA van medewerkers. Evenwel is de manier waarop training hierover gegeven wordt van groot belang. In hun onderzoek stellen Öğütçü et al. (2016) vast: "One of the most significant findings of this study is that the higher the education level, the more their information security awareness is." Er is dus een positieve correlatie gevonden tussen opleidingsniveau en ISA. Dit onderzoek is echter uitgevoerd bij studenten, academici en medewerkers van een universiteit.

1.3. Probleemstelling

In de literatuur wordt een aantal keer kennis en of opleiding in verband gebracht met gedrag ten opzichte van ISA. Maar hoe verhoudt zich dit bij een bedrijf in de profit sector? En met name bij niet technische gebruikers ofwel gebruikers die professioneel gezien niet met Infosec issues bezig zijn.

Vanuit de bevindingen in de vorige paragraaf kom ik voor mijn onderzoek tot de volgende probleemstelling.

Probleemstelling:
Organisaties zoeken al jaren naar manieren om de ISA van hun medewerkers te verhogen. Door onderzoek zijn inmiddels diverse factoren bekend die van invloed zijn op ISA. Organisaties kunnen deze factoren gebruiken voor de invulling van organisatorische en educatieve maatregelen, om de ISA van hun medewerkers te vergroten en daarmee Infosec risico's te verlagen. Uit onderzoek wordt voor alsnog niet duidelijk of opleidingsniveau één van de factoren is, die van invloed is op ISA.

1.4. Opdrachtformulering

Deze studie heeft als doel onderzoek te doen naar de relatie tussen opleidingsniveau en Information Security Awareness (ISA). Resultaten kunnen mogelijk een bijdrage leveren aan de verklaring van de variatie in ISA bij werknemers, in relatie tot de hoogte van de opleiding maar ook het soort opleiding. Hebben bijvoorbeeld mensen met een IT-opleiding een hogere ISA dan mensen zonder IT-opleiding? En hoe vertaalt zich dat het best naar de educatieve benadering van ISA door een werkgever? En dient educatie gericht te zijn op het verhogen van kennis, de houding van werknemers of juist hun gedrag.

Onderzoeksvraag: Is er een verband tussen opleidingsniveau en ISA op de onderdelen kennis, houding en gedrag voor non-technical users in een profit organisatie?

Subvragen van het onderzoek:

- Kennen medewerkers met een hogere opleiding de regels beter of slechter dan mensen met een lagere opleiding?
- Begrijpen medewerkers met een hogere opleiding beter of slechter waarom ze zich aan de regels moeten houden dan mensen met een lagere opleiding?
- Gedragen medewerkers met een hogere opleiding zich meer of minder in lijn met de regels en wat er van ze verwacht wordt dan mensen met een lagere opleiding?

Het onderzoek is opgesplitst in een literatuuronderzoek en een empirisch onderzoek.
Het literatuuronderzoek is er op gericht om na te gaan of er theorieën bekend zijn die gaan over het verband tussen opleidingsniveau en ISA. Vragen hierbij zijn:

- Is er literatuur bekend over het verband tussen opleidingsniveau en ISA?
- Toont deze literatuur dit verband aan of juist niet?
- Wordt hierbij nog specifiek verwezen naar een verband met kennis, houding of gedrag van ISA?

In het empirische onderzoek zullen de bevindingen uit het literatuuronderzoek worden getoetst in de praktijk, waarbij antwoord wordt gezocht op de volgende vragen:

- Leidt een hogere opleiding tot een hogere ISA?
- Zo niet, heeft enig opleidingsniveau een significant hogere ISA?
- Leidt een hogere opleiding tot een hogere kennis van ISA?
- Zo niet, heeft enig opleidingsniveau een significant hogere kennis van ISA?
- Leidt een hogere opleiding tot een betere houding t.o.v. ISA?
- Zo niet, heeft enig opleidingsniveau een significant betere houding t.o.v. ISA?
- Leidt een hogere opleiding tot een beter gedrag in het kader van ISA?
- Zo niet, heeft enig opleidingsniveau een significant beter gedrag in het kader van ISA?
- Leidt een IT-opleiding tot een hogere ISA?
- Leidt een IT-opleiding tot een hogere kennis van ISA?
- Leidt een IT-opleiding tot een betere houding t.o.v. ISA?
- Leidt een IT-opleiding tot een beter gedrag in het kader van ISA?

Met het antwoord op deze vragen kan de vraag beantwoord worden, of er een relatie is tussen opleidingsniveau en de verschillende onderdelen van ISA en ISA in het algemeen. Daarnaast kan de vraag beantwoord worden of een specifiek opleidingsniveau een hogere ISA heeft. Tenslotte kan de vraag beantwoord worden of een IT-opleiding tot een hogere ISA leidt.

1.5. Motivatie / relevantie

De wetenschappelijk toegevoegde waarde van het onderzoek is dat het een beeld geeft van de relatie tussen opleidingsniveau en ISA van medewerkers.
De maatschappelijke relevantie is, dat indien er een significante relatie bestaat tussen opleidingsniveau en ISA, dat een organisatie zijn educatieve maatregelen om ISA te verhogen dan kan afstemmen op het opleidingsniveau van een medewerker. Opleidingsniveau is namelijk eenvoudig vast te stellen in tegenstelling tot specifieke persoonskenmerken die ISA beïnvloeden. Indien kennis, houding of gedrag per opleidingsniveau verschilt dan kan een bedrijf er bijvoorbeeld voor kiezen om mensen met een lage opleiding meer kennis bij te brengen en bij mensen met een hoge opleiding training te geven op het gebied van gedrag. Als verder uit het onderzoek blijkt dat een IT-opleiding leidt tot een hogere ISA, dan kan een organisatie medewerkers een IT- training laten volgen om de ISA te verhogen.

1.6. Aanpak in hoofdlijnen

Het rapport is als volgt gestructureerd. In hoofdstuk 1 staat de introductie. Het theoretische kader op basis van de gevonden literatuur wordt in hoofdstuk 2 behandeld. Hoofdstuk 3 beschrijft de methodologie van het onderzoek. De resultaten van het onderzoek en de interpretatie daarvan worden in hoofdstuk 4 beschreven. Hoofdstuk 5 bevat tenslotte de conclusies.

2. Theoretisch kader

In dit hoofdstuk wordt de totstandkoming van het theoretisch kader uiteen gezet.

2.1. Onderzoeksaanpak

Op de volgende vragen moet vanuit de wetenschappelijke literatuur een antwoord worden gevonden:

- Is er literatuur bekend over het verband tussen opleidingsniveau en ISA?
- Toont deze literatuur dit verband aan of juist niet?
- Wordt hierbij nog specifiek verwezen naar een verband met kennis, houding of gedrag van ISA?

Om literatuur te vinden die antwoord op de onderzoeksvragen zou kunnen geven, worden termen uit deze vragen gecombineerd en als zoekterm ingevoerd in Quick search van de OU bibliotheek. Op die manier wordt gezocht naar literatuur in alle beschikbare databases. Er zijn een aantal query's gemaakt waarin de termen ISA, opleiding, kennis, houding en of gedrag zijn gecombineerd tot zoekacties. Hoe de query's precies zijn bepaald staat beschreven in bijlage 1. De zoektermen zijn waar nodig vertaald naar de Engelse taal. Bij deze query's is in alle gevallen geselecteerd op taal Engels en peer reviewed literatuur van maximaal 15 jaar oud. Voor maximaal 15 jaar oud is gekozen, omdat uit hoofdstuk 1 is gebleken dat veel ontwikkelingen op het gebied van ISA in de laatste 10 à 15 jaar hebben plaats gevonden.

In de volgende paragraaf wordt beschreven hoeveel resultaten dit heeft opgeleverd per query, hoeveel na filtering, hoeveel er bekeken zijn en hoeveel er uiteindelijk zijn geselecteerd.

2.2. Uitvoering

Er is in de literatuur gezocht naar aanwijzingen voor de invloed van opleidingsniveau op ISA en de deelgebieden van ISA. Met als doel om uiteindelijk antwoord de kunnen geven op de onderzoeksvragen van het literatuuronderzoek. Hiertoe zijn een aantal query's gemaakt, waarna een selectie van literatuur heeft plaats gevonden. Hoe dat is gedaan, staat beschreven in bijlage 1. In deze paragraaf worden de resultaten van de query's en verdere selectie gepresenteerd.

Totaaloverzicht van de resultaten:

Query	aantal resultaten	aantal bekeken	aantal relevant	inclusief literatuurlijst en citaten onderzoek
1	32	-	-	-
2	59	-	-	-
3	39	25	7	11

Tabel 1: Totaaloverzicht resultaten literatuuronderzoek

De 11 resultaten die als bron worden gebruikt voor het literatuuronderzoek, zijn geselecteerd omdat hierin aanwijzingen zijn gevonden die een bijdrage kunnen leveren aan het antwoord op de onderzoeksvragen van het literatuuronderzoek. Dit wordt in paragraaf 2.3 verder uiteen gezet.

Bijlage 2 is het totaaloverzicht van de resultaten van de query's, de gelezen literatuur, de relevante literatuur en literatuur die is toegevoegd na literatuurlijst- of citatieanalyse. De relevante artikelen worden in de literatuurlijst opgenomen. In de volgende paragraaf wordt beschreven welke resultaten het bestuderen van de relevante artikelen heeft opgeleverd.

2.3. Resultaten en conclusies

In deze paragraaf staat het ontwikkelde theoretisch kader: de antwoorden (voor zover gevonden) op de gestelde vragen met de argumenten die, op basis van gevonden literatuur, tot deze antwoorden heeft geleid.

De invloed van opleidingsniveau op ISA is in de afgelopen 10 jaar meerdere malen onderzocht. Vaak als bijvangst van een onderzoek en een enkele keer als concreet onderwerp. Vooral in eerdere onderzoeken wordt geen significante invloed van opleidingsniveau op ISA gevonden. Zoals bij Bulgurcu, Cavusoglu, and Benbasat (2010), die een stelling onderzochten: hoe hoger het niveau van opleiding en kennis van technologie van een medewerker, des te groter hun intentie om te voldoen aan het Information security beleid. Dit werd niet bevestigd. Ook in het onderzoek van Pattinson, Butavicius, Parsons, McCormac, and Calic (2015) is, in tegenstelling tot wat zij verwacht hadden, geen positief verband gevonden tussen opleidingsniveau en Infosec gedrag. Zij hadden verwacht dat mensen met een hogere opleiding zich meer bewust zouden zijn van de consequenties van serieuze security doorbraken en zich daardoor beter c.q. verantwoordelijker zouden gedragen. Hoewel recenter, is ook in het onderzoek van Kiss (2019) geen invloed van opleidingsniveau op ISA gevonden. Er werd onderzocht of er een significante toename van ISA was gedurende de looptijd van een academische studie. Omdat dit echter binnen één en dezelfde studie gemeten is, zegt dit misschien meer over de studie zelf dan over de invloed van de hoogte van het opleidingsniveau op ISA.

Verschillende onderzoeken hebben positieve correlaties gevonden tussen opleidingsniveau op ISA, hoewel niet altijd heel concreet of goed onderbouwd. Zoals bij McCormac, Zwaans, et al. (2017), dat factoren als opleiding en Infosec training ook invloed kunnen hebben op ISA. In het onderzoek wordt geen onderbouwing voor deze stelling gevonden. Volgens Wiley, McCormac, and Calic (2020) is er een positieve correlatie tussen hogere ISA en individuen met een hoger opleidingsniveau. Zij verwijzen hierbij naar 3 studies namelijk die van McCormac (2018), Pattinson (2016) en Shrobshire (2006). Na bestudering van deze onderzoeken, kan nergens deze concrete bevinding worden terug gevonden. Verdere aanwijzingen zijn gevonden in het onderzoek van Parsons et al. (2014). Zij zeggen: “Employers can be relatively confident that improving their employees' knowledge of policy and procedures will have a positive impact on both attitude towards those policies and procedures and employee behaviour.” Dit zegt iets over de deelgebieden van ISA onderling, namelijk dat kennis van procedures invloed heeft op houding en gedrag. Maar niet dat opleidingsniveau invloed heeft op ISA of op de deelgebieden kennis, houding en gedrag.

Gebruikers van information systems hebben door hun verschillend beroep en verschillende opleidingsachtergrond een verschillend niveau van security awareness (Aydın & Chouseinoglou, 2013). Hoewel verschillende opleidingen een verschillende mate van security awareness hebben, wordt niet duidelijk of een hoger opleidingsniveau een hogere awareness tot gevolg heeft. Latere onderzoeken tonen heel concreet een positieve correlatie aan tussen opleidingsniveau en ISA. Opleidingsniveau en Infosec awareness hebben een positieve correlatie (Öğütçü et al., 2016). Leeftijd, werkgebied en opleidingsniveau hebben een significant effect op ISP awareness en de naleving ervan (Chua, Wong, Low, & Chang, 2018). Met name de opmerking over de naleving is hier ook interessant. Dat zegt namelijk iets over een significant effect van opleidingsniveau op nakoming van de regels c.q. gedrag. Bovendien betreft het hier werknemers in organisaties, dus zeer treffend voor dit onderzoek.

In de bestudeerde literatuur is ook informatie gevonden waarin wordt verwezen naar een verband m.b.t. kennis, houding of gedrag ten opzichte van ISA. Uit het onderzoek van Stanton, Mastrangelo,

Stam, and Jolton (2004) zou je kunnen concluderen dat hoger opgeleiden gedrag vertonen dat beter in lijn is met ISA . Zij komen namelijk tot de bevinding dat: “Those with higher incomes reported better password management practices and less password sharing than those with lower incomes.” Alleen als je veronderstelt dat een hoger inkomen in verband staat met een hogere opleiding, kun je tot de conclusie komen dat hoger opgeleiden beter omgaan met hun passwords in de zin van Infosec en dus een hoger ISA hebben. Hoger opgeleiden hebben een hogere ISA op het gebied van gedrag (Aydın & Chouseinoglou, 2013). Deze conclusie kan getrokken worden uit het onderzoek, waarin artsen werden onderzocht in hun omgang met gevoelige informatie. Algemeen samengevat hadden de hoger opgeleiden in dit onderzoek een meer risico ontwijkende houding, dus een hogere ISA op het specifieke onderdeel houding. Dit in tegenstelling tot wat Šolić, Pleša, Velki, and Nenadić (2019) hebben vastgesteld dat mensen met een lagere opleiding een bewustere houding hebben tegenover bepaalde Infosec onderwerpen. De conclusies van deze laatste twee onderzoeken, beiden op het gebied van Healthcare, spreken elkaar dus tegen.

In bijlage 3 staat een overzicht van alle stellingen die gevonden zijn in de bronnen van het literatuuronderzoek.

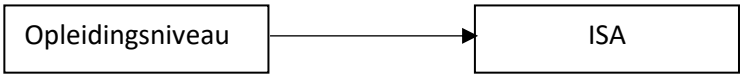
Hieruit kunnen een aantal conclusies worden getrokken m.b.t. de onderzoeksvragen. Het literatuuronderzoek toont aan dat er diverse literatuur bekend is over het verband tussen opleidingsniveau en ISA. In enkele gevallen is geen positieve correlatie gevonden en enkele keren is er wel significante positieve correlatie gevonden. Wat opvalt is dat de onderzoeken die wel een significante positieve correlatie hebben gevonden tussen opleidingsniveau en ISA de meest recente onderzoeken zijn, namelijk uit 2016 en 2018. In tegenstelling tot de onderzoeken die geen significante correlatie hebben gevonden, welke stammen uit 2010 en 2015. Waardoor dit komt is onbekend. Er wordt af en toe specifiek verwezen naar een correlatie tussen houding of gedrag en ISA. Er is geen literatuur gevonden die de correlatie tussen opleidingsniveau en kennis van ISA beschrijft. Drie keer wordt gesproken over een positieve correlatie tussen opleidingsniveau en houding of gedrag ten opzichte van ISA, één keer zouden lager opgeleiden juist een bewustere houding hebben.

In de volgende paragraaf worden de consequenties, naar aanleiding van de uitkomst van het literatuuronderzoek, voor het vervolg van het onderzoek uiteen gezet.

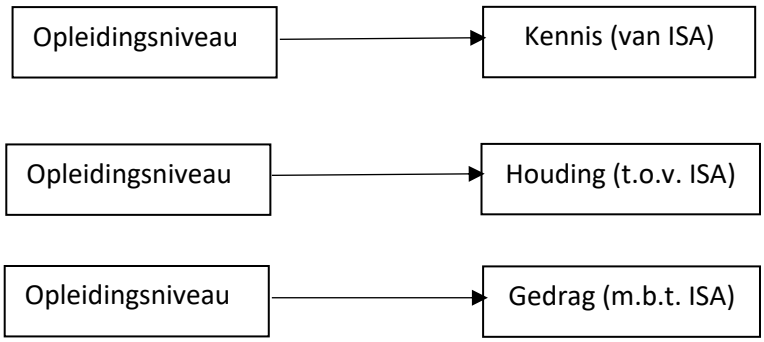
2.4. Doel van het vervolgonderzoek

Op basis van de resultaten van het literatuuronderzoek, wordt de stelling aangenomen dat opleidingsniveau van invloed is op ISA. Meerdere recente onderzoeken tonen een significante positieve correlatie aan. Niet het enige maar wel het meest concreet is het onderzoek van Chua et al. (2018), wat behalve een significant effect van opleidingsniveau op ISP awareness, tevens een significant effect aantoont van opleidingsniveau op nakoming van de regels en dus gedrag. Het onderzoek is zeer recent en gaat bovendien over werknemers in organisaties, waar ook de onderzoeksvraag van het huidige onderzoek over gaat.

De hypothese vanuit het literatuuronderzoek is dan ook dat er een verband is tussen opleidingsniveau en ISA. In het empirisch onderzoek zal onderzocht worden, of deze stelling wordt bevestigd.



Het empirisch onderzoek zal daarnaast gericht zijn op het beantwoorden van de drie sub-vragen van het onderzoek, inzake de invloed van opleidingsniveau op de onderdelen kennis, houding en gedrag van ISA. Het literatuuronderzoek heeft deze vragen slechts deels beantwoord. Alleen Chua et al. (2018) hebben aangetoond dat opleidingsniveau significant effect heeft op nakoming van de regels, ofwel op het gedrag. Verdere concrete aanwijzingen zijn niet aangetroffen, waardoor deze vragen in het empirisch onderzoek beantwoord dienen te worden. Bij aanvang van het empirisch onderzoek wordt evenwel de stelling ingenomen dat opleidingsniveau van invloed is op de ISA onderdelen kennis, houding en gedrag. De onderstaande hypothesen zullen daartoe in het empirisch onderzoek getoetst moeten worden:



Als er geen invloed van het opleidingsniveau op ISA of de onderdelen van ISA kan worden gevonden, dan zal getoetst worden of enig opleidingsniveau een hogere ISA heeft, of dat enig opleidingsniveau een hogere kennis, betere houding of beter gedrag heeft. Tenslotte zal worden onderzocht of een IT-opleiding leidt tot een hogere ISA, een hogere kennis, betere houding of beter gedrag. Daartoe worden de hypothesen zoals hierboven getoond nogmaals getoetst waarbij opleidingsniveau vervangen wordt door IT-opleiding.

De ISA van de medewerkers dient gemeten te worden, om antwoord op de onderzoeksvragen te krijgen. In hoofdstuk 3 wordt beschreven welke onderzoeksmethode hiervoor gebruikt zal worden. Het wetenschappelijke doel van het vervolgonderzoek is het vergroten van het inzicht in de relatie tussen opleidingsniveau en ISA. Het maatschappelijke doel van het onderzoek is dat door dit inzicht een organisatie zijn educatieve maatregelen om ISA te verhogen dan kan afstemmen op het opleidingsniveau van een medewerker. Dit kan bijdragen aan een verhoging van ISA en daarmee een verlaging van de Infosecurity risico’s.

3. Methodologie

In dit hoofdstuk vindt verantwoording plaats voor de uitvoering van het empirische onderzoek.

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode

In deze paragraaf wordt beschreven met argumenten hoe het onderzoek zal plaats vinden.

Het empirisch onderzoek heeft tot doel om de hypotheses zoals uiteen gezet in paragraaf 2.4 te toetsen en daarmee een mogelijk positieve correlatie vast te stellen tussen opleidingsniveau en hoogte van ISA bij werknemers in een profit organisatie. Specifiek non-technical users, zoals in de onderzoeksvraag omschreven. De hypotheses worden getoetst door het verzamelen van toepasselijke data en deze wordt vervolgens geanalyseerd. Als de geanalyseerde resultaten consistent zijn met de hypotheses, dan zijn de hypotheses bevestigd. Zo niet dan worden zij verworpen.

Om de hypothesen te kunnen toetsen, is informatie nodig over de ISA van werknemers in een profit-organisatie, specifiek de kennis van ISA, houding t.o.v. ISA en gedrag m.b.t. ISA. Daarnaast is informatie over het opleidingsniveau van die medewerkers benodigd en het feit of medewerkers een IT-opleiding hebben gevolgd. De IT-opleiding kan overigens een aparte opleiding zijn, anders dan de hoogst genoten opleiding. Uitgaande van eigen waarnemingen voor empirisch onderzoek, zal de benodigde informatie bij werknemers in een organisatie bevraagd moeten worden. De onderzoeksstrategie is de case study. De caseorganisatie is de organisatie waar de onderzoeker werkzaam is. Werknemers binnen deze organisatie zullen benaderd moeten worden voor het onderzoek.

De aard van het onderzoek is theoretisch gezien deductief. Bij dit type onderzoek worden hypotheses vastgesteld na het lezen van academische literatuur, waarbij een onderzoekaanpak wordt opgezet om deze te toetsen in een specifieke situatie. Deductief onderzoek stelt je in staat om relaties tussen variabelen te onderzoeken en uit te leggen. Daarbij worden feiten gemeten, vaak kwantitatief en is het van belang om de steekproef zorgvuldig en voldoende groot te kiezen, om aan de hand van de onderzoeksresultaten uitspraken te kunnen doen over de gehele populatie (Saunders, Lewis, & Thornhill, 2016). Gezien de aard van de onderzoeksvragen en de methode, moet er in de korte tijd van het onderzoek veel data verzameld worden bij een grote groep mensen over verschillende feiten, zoals de hoogte van de ISA van de medewerkers. Observatie of gestructureerde of semigestructureerde interviews zijn minder geschikt om veel verschillende feiten te verzamelen bij een grote groep mensen en bovendien zou dit gezien de tijd en de middelen die beschikbaar zijn ook niet haalbaar zijn. Gestandaardiseerde vragenlijsten werken het best, omdat je ervan op aan kunt dat ze op dezelfde manier geïnterpreteerd worden door alle respondenten (Saunders et al., 2016). Door middel van vragenlijsten kan gestandaardiseerde data verzameld worden van een aanzienlijke populatie op een hele economische manier, waarbij vergelijken gemakkelijk wordt (Saunders et al., 2016). Om het verzamelen en verwerken van de data door middel van statistische methoden te vergemakkelijken wordt een online enquête uitgezet. In de volgende paragraaf wordt besproken welke standaard vragenlijst gebruikt zal worden voor het onderzoek.

3.2. Technisch ontwerp: uitwerking van de methode

In deze paragraaf worden de details van de uitvoering van het onderzoek besproken.

Zoals in de vorige paragraaf besproken zal de benodigde data voor het empirisch onderzoek worden verzameld door middel van een vragenlijst. De vragenlijst die gebruikt wordt is gebaseerd op een standaard methode, de HAIS-Q vragenlijst. De complete HAIS-Q vragenlijst staat in bijlage 4. Deze

vragenlijst is speciaal ontwikkeld door Parsons et al. (2017) om de hoogte van de ISA vast te stellen van een populatie op het gebied van kennis, houding en gedrag. Ten eerste zijn dit exact de onderdelen van ISA die hier onderzocht moeten worden, getuige de onderzoeksvraag: Is er een verband tussen opleidingsniveau en ISA op de onderdelen kennis, houding en gedrag voor non-technical users in een profit organisatie? Ten tweede hebben 2 studies bevestigd dat de HAIS-Q methode statistisch gezien een valide methode is om ISA te meten en daarnaast, dat de methode Information security gedrag kan voorspellen (Parsons et al., 2017). Het voorspellen van gedrag kan met name interessant zijn voor educatieve doeleinden.

De HAIS-Q vragenlijst bestaat uit 63 vragen die zeven aandachtsgebieden beoordeelt, namelijk wachtwoordbeheer, e-mailgebruik, internetgebruik, gebruik van social media, mobiele apparaten, informatieverwerking en incidentrapportage. Elk aandachtsgebied is verder onderverdeeld in drie specifieke gebieden, resulterend in 21 aandachtsgebieden, die elk worden gemeten via een apart kennis-, houding- en gedragsitem. Binnen iedere set vragen, worden alle items gepresenteerd in een vaste willekeurige volgorde en 32 van de 63 items zijn negatief verwoord (aangegeven met ^ in bijlage 4). Door vragen in een willekeurige vaste volgorde te zetten is er minder kans dat vragen met elkaar in verband worden gebracht waardoor deze hetzelfde beoordeeld zouden worden. Het negatief verwoorden van een aantal vragen, maakt dat de respondent telkens opnieuw over zijn antwoord moet nadenken. Respondenten wordt gevraagd om te antwoorden door middel van een Likert schaal van 1 tot 5, variërend van “Sterk mee oneens” tot “Sterk mee eens”. Er wordt een schaal geconstrueerd om een ISA score vast te stellen op basis van de antwoorden, zoals ook gedaan is door Parsons et al. (2014). Ieder antwoord wordt gewaardeerd met een score van 1 tot 5. De negatieve vragen worden her gecodeerd zodat bij elke vraag een lage score een lage ISA inhoudt en een hoge score een hoge ISA. Hetzelfde wordt gedaan voor de onderdelen kennis, houding en gedrag. Het resultaat van deze schaal is een gemiddelde ISA-score per respondent voor alle 63 vragen. Zonder er een waardeoordeel aan te verbinden zoals goed of slecht, kun je de scores dan vergelijken en aangeven of een bepaalde opleiding een hogere ISA score heeft dan een andere op de gegeven schaal.

Specifiek voor dit onderzoek wordt een aantal extra gegevens gevraagd aan de respondenten, namelijk het opleidingsniveau volgens het Nederlands kwalificatieraamwerk (NLQF) in bijlage 7 en of er een IT-opleiding gevolgd is. De HAIS-Q vragenlijst wordt voor het onderzoek vertaald in de Nederlandse taal. Aangezien de populatie ook Nederlands is, wordt dan een beter begrip van de vragen verwacht en een betere response (Saunders et al., 2016). Bij het vertalen wordt rekening gehouden met de exacte betekenis van individuele woorden, combinaties van woorden en de volgorde van woorden. In bijlage 5 staan alle vragen vertaald in het Nederlands en verdeeld in de onderdelen kennis, houding en gedrag.

De vragenlijst is een zogenaamde self completed vragenlijst, die medewerkers zelf zullen invullen en die via het internet wordt aangeboden. De uitnodiging hiervoor zal per e-mail verzonden worden naar de medewerker, die vervolgens door op een link te klikken de vragenlijst kan starten. In de uitnodiging wordt het belang van het invullen, in het kader van het onderzoek maar ook voor de werkgever, van de vragenlijst beschreven en de benodigde tijd die hiervoor nodig is. Voor het invullen van de vragenlijst krijgen de respondenten een korte instructie. Daarna worden de onderdelen kennis, houding en gedrag afzonderlijk en achtereenvolgens gepresenteerd, met specifieke instructies die deze onderdelen beschrijven. Direct daarop volgend start de vragenlijst.

De medewerkers zijn zelf voor alle data de bron waar de informatie vandaan wordt gehaald. Informatie over opleidingen wordt bijvoorbeeld niet gevraagd aan de afdeling HRM van de case organisatie, omdat dan de namen van de geënquêteerden bekend wordt. Terwijl het juist de

bedoeling is dat de enquête anoniem is, om de kans op sociaal wenselijke antwoorden te verkleinen. Daarom zal alle informatie bij medewerkers zelf worden gevraagd, waarbij zij zelf anoniem blijven.

Medewerkers die worden betrokken bij het onderzoek, moeten voldoen aan de volgende eisen:

- Medewerkers moeten in dienst zijn bij de case organisatie
- Medewerkers zijn kantoormedewerkers met een computer/laptop van het werk
- Medewerkers werken niet op de afdeling Information security

Het onderzoek zal plaats vinden bij Sligro Foodgroup B.V. te Veghel. Bij dit bedrijf is navraag gedaan of men een bepaald beeld heeft van de ISA van medewerkers maar dit is nooit eerder gemeten. Voor de case organisatie zal dit onderzoek daarom een nulmeting van de ISA zijn.

Om een algemene uitspraak te kunnen doen over een verband tussen het opleidingsniveau en de ISA van de medewerkers in de case organisatie, zal de gehele populatie bevraagd moeten worden of anders zal een representatieve en statistisch gezien voldoende grote steekproef uit een populatie genomen moeten worden. Daarnaast moeten van alle verschillende afdelingen medewerkers betrokken worden in het onderzoek voor voldoende diversiteit. De exacte invulling zal met de case organisatie besproken worden. De populatie voor het onderzoek zijn alle kantoormedemerkers van de case organisatie, daarbij rekening houdend met de eisen zoals hierboven gesteld. Dit overzicht staat in bijlage 6. Zo vallen medewerkers van de kantine en facilitaire dienst af, omdat zij geen computer gebruiken. IT medewerkers die vallen onder de afdeling Security vallen ook af. “HK uitzonderlijk personeel”, zijn wel in dienst maar niet werkzaam, bijvoorbeeld langdurig zieken, en worden dus ook niet meegerekend. De definitieve populatie zal in overleg met de organisatie worden vastgesteld.

3.3. Gegevensanalyse

In deze paragraaf volgt een beschrijving en onderbouwing hoe de te verzamelen gegevens geanalyseerd zullen worden. Met welke methoden en welke voor- en nadelen dit met zich mee brengt.

Gegevensanalyse bestaat uit een aantal stappen:

- Voorbereiden van de data, invoer in een computer en controleren van de data
- Selecteren van toepasselijke tabellen en grafieken om de data te presenteren
- Selecteren van toepasselijke statistische methoden om de data te beschrijven
- Selecteren van toepasselijke statistische methoden om relaties en trends in je data te onderzoeken

Er zijn verschillende soorten data die vastgelegd worden in het onderzoek. De antwoorden op de HAIS-Q vragen zijn ordinaal data. Data over het opleidingsniveau is ordinaal. IT-opleiding is dichotome data, immers is het antwoord ja of nee. De data wordt vastgelegd in tabel vorm, een zogenaamde data matrix en ge-upload in SPSS statistics, al waar het wordt opgeslagen. Daarbij vertegenwoordigen de kolommen de variabelen en de rijen de waarden. Nadat de data is opgeslagen zullen verschillende bewerkingen op de data worden gedaan.

Alvorens data te analyseren in SPSS, worden de gegeven antwoorden globaal onderzocht om de datakwaliteit te beoordelen. Hierbij zullen, net zoals Parsons et al. (2017) zelf hebben gedaan, de richtlijnen van Meade and Craig (2012) worden geraadpleegd. Deze richtlijnen bevatten tips voor het herkennen van non-responsiviteit van inhoud, wat helpt bij het identificeren van antwoorden die onzorgvuldig gegeven zijn. Bijvoorbeeld respondenten die bij alle antwoorden “Sterk mee eens”

hebben ingevuld. Op het moment dat dit geconstateerd wordt kunnen de betreffende ingevulde vragenlijsten komen te vervallen.

De volgende controles uit Meade and Craig (2012) worden toegepast:

- Controle op patronen van steeds hetzelfde antwoord
- Controle op patronen die zich herhalen maar waarbij antwoorden ongelijk zijn

De verzamelde gegevens worden vervolgens ingevoerd in SPSS statistics om gepresenteerd, beschreven en geanalyseerd te worden. Allereerst wordt de ISA score berekend voor ISA totaal, kennis, houding en gedrag zoals beschreven in paragraaf 3.2. Door middel van tabellen en grafieken wordt de data gepresenteerd. Dan volgen beschrijvende statistieken zoals gemiddelde, meest voorkomende waarde, spreiding en variantie. Tenslotte worden relaties, verschillen en trends onderzocht in de data. Het meest interessant is om te weten hoe een variabele zich verhoudt tot een andere variabele, hoe significant en hoe sterk deze verhouding is. De variabelen die hiervoor met name in aanmerking komen zijn het opleidingsniveau en de hoogte van ISA. Nadat deze analyse heeft plaatst gevonden kunnen de vragen van het empirische onderzoek worden beantwoord.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

In deze paragraaf wordt de manier waarop het onderzoek is opgezet verantwoord, qua validiteit en betrouwbaarheid.

Betrouwbaarheid van het onderzoek hangt samen met replicatie en consistentie. Dat wil zeggen, dat als hetzelfde onderzoek nogmaals wordt uitgevoerd op de besproken manier, dat dan dezelfde bevindingen worden gedaan. Een hoge mate van structuur om replicatie mogelijk te maken is een belangrijk onderwerp om betrouwbaarheid te verzekeren. Daarom is onder andere gekozen voor een standaard vragenlijst. De HAIS-Q vragenlijst is, zoals in paragraaf 3.2 beschreven, statistisch gezien een valide methode om ISA te meten. Interne validiteit is hiermee geborgd, waardoor men ervan uit kan gaan dat de uitkomsten van deze vragenlijst een goed beeld geven van de ISA van de werknemers van de organisatie. Verder zal door design van de vragen, een duidelijke en mooie presentatie, heldere uitleg van het doel en zorgvuldige planning en uitvoering van aanlevering en retournering van vragenlijsten de betrouwbaarheid worden verhoogd. Pilot testing kan hier ook aan bijdragen maar wordt in principe niet gedaan, omdat dit veel tijd kost en die niet beschikbaar is.

Een zwak punt van de methode is dat de vragenlijst door de personen zelf wordt ingevuld. Je bent afhankelijk van het eerlijk invullen door de geënquêteerden. Sociaal wenselijke antwoorden komen voort uit het feit dat mensen geneigd zijn zichzelf op een zo goed mogelijke manier te presenteren (McCormac, Calic, et al., 2017). Dit kan leiden tot een scheef beeld van de resultaten en bevindingen. Dit moet zo goed mogelijk worden ondervangen. McCormac, Calic, et al. (2017) komen tot de bevinding dat het verzekeren van anonimiteit en vertrouwelijkheid van respondenten, de neiging tot het geven van sociaal wenselijke antwoorden kan verkleinen. Daarnaast draagt deze zekerheid volgens hen bij aan het geven van meer waarheidsgetrouwe antwoorden. De respondenten zal daarom niet gevraagd worden om hun naam te vermelden en in de introductie van de vragenlijst zal de anonimiteit extra worden benadrukt. Hierdoor zou het geven van sociaal wenselijke antwoorden verminderd moeten worden, zegt ook Parsons et al. (2014). Ook wordt niet gevraagd naar de leeftijd van de medewerkers, omdat leeftijd in relatie tot ISA al eerder onderzocht is (Chua et al., 2018; McCormac, Zwaans, et al., 2017). Dit draagt ook bij aan de verhoging van de betrouwbaarheid van de data.

Een vraag in de HAIS-Q vragenlijst is aangepast. Het betreft de volgende vraag: “Ik controleer dat vreemden mijn laptopscherm niet kunnen zien, als ik aan een gevoelig document werk.” De kern van de vraag is hier het meekijken door vreemden. Het risico van meekijken door vreemden is niet alleen van toepassing bij laptopgebruik maar geldt voor alle schermen waar gevoelige informatie op kan worden getoond. Het woord laptopscherm wordt daarom vervangen door scherm. Hierdoor koppel je het risico los van het gebruik van een specifiek apparaat en wek je niet de suggestie dat de vraag voor iemand niet bestemd zou zijn. Er zijn nog twee vragen m.b.t. gebruik van een laptop. Een vraag gaat over gebruik in openbare ruimten. De andere vraag gaat over het onbeheerd achter laten van de laptop. Respondenten die niet over een laptop beschikken krijgen bij deze vragen de mogelijkheid om dit aan te geven door de keuzemogelijkheid “ik werk niet op een laptop.”

De validiteit van het onderzoek kan niet worden verhoogd door triangulatie of participant validatie. Het onderzoek is namelijk een enkelvoudig onderzoek door middel van een vragenlijst en daarnaast is het anoniem. Er kan daarom niet bij respondenten gevalideerd worden of de data correct is ingevuld. Achteraf kunnen op basis van de richtlijnen van Meade and Craig (2012) bepaalde vragenlijsten worden verwijderd die als sociaal wenselijk of onzorgvuldig ingevuld worden beschouwd. Dit draagt echter niet bij aan het voorkomen van sociaal wenselijke antwoorden. Bij de HAIS-Q vragenlijst moet altijd een antwoord worden gegeven. Of antwoorden legitiem zijn kan hier echter niet beoordeeld worden, omdat het om persoonlijke gegevens, kennis en gedrag gaat.

Indien een steekproef wordt genomen voor het empirisch onderzoek, dient dit met zorg te gebeuren in verband met externe validiteit. Om namelijk uitspraken over de gehele populatie te kunnen doen, moeten alle afdelingen voldoende vertegenwoordigd zijn. Er zijn hele kleine en hele grote afdelingen bij de gekozen organisatie waardoor het kiezen van de steekproef erg belangrijk is. Wellicht wordt ervoor gekozen om de gehele populatie te bevragen maar dan moet er nog op gelet worden dat bij de response alle afdelingen betrokken zijn.

Het is van belang dat medewerkers ten eerste van het bedrijf ook te horen krijgen dat het onderzoek belangrijk is en daarnaast dat zij ruim de tijd krijgen, binnen werktijd, om de vragenlijst in te vullen. Het is belangrijk dat de leidinggevenden van de werknemers achter het onderzoek staan en dit ook zo uitdragen. Dit vergroot de response maar ook de betrouwbaarheid.

Er is voor gekozen om in plaats van te vragen naar de hoogst genoten opleiding, te vragen naar de laatst genoten opleiding. Lager opgeleiden zouden de vraag naar de hoogst genoten opleiding als neerbuigend of discriminerend kunnen opvatten.

4. Resultaten

In dit hoofdstuk worden de resultaten van het onderzoek beschreven en wordt antwoord gegeven op de vragen van het empirische onderzoek. De vragen van het empirische onderzoek worden behandeld in aparte paragrafen. Ook zal worden aangegeven waar afwijkingen van het oorspronkelijke plan van aanpak optraden, zoals omschreven in hoofdstuk 3.

Respondenten zijn vastgesteld op basis van de richtlijnen in paragraaf 3.2. Er is in overleg met de caseorganisatie besloten om op basis van deze richtlijnen de gehele populatie van de caseorganisatie in de enquête mee te nemen. Het was verder de keuze van de caseorganisatie om directie en topmanagement uit te sluiten van deelname. Via een interne query zijn de e-mailadressen van de respondenten achterhaald en geladen in Limesurvey. In totaal zijn 726 uitnodigingen verzonden om aan de enquête deel te nemen. De enquête startte op maandag 7 december en eindigde op maandag 21 december 2020. Gedurende de looptijd is tweemaal een herinnering verstuurd. De eerste keer na een week en de tweede keer op de voorlaatste dag. Deze herinneringen hebben zo'n 110 extra responsen opgeleverd. In totaal waren er 457 responsen, waarvan 362 volledig en 95 volledig. De 362 volledige ingevulde vragenlijsten vertegenwoordigen 50% responsegraad, waardoor besloten is om de onvolledig ingevulde responsen niet verder mee te nemen in het onderzoek.

In de volgende paragraaf staat beschreven hoe de data is voorbereid op verwerking in SPSS. In paragraaf 4.2, 4.3 en 4.4 worden de resultaten beschreven uitgewerkt per deelvraag van het onderzoek.

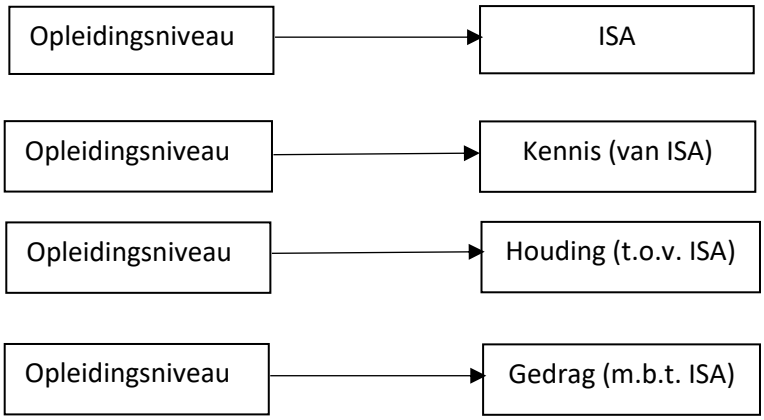
4.1. Voorbereiding data

De ruwe data is gecontroleerd op non-responsiviteit. Hierbij zijn regels van Meade and Craig (2012) gebruikt zoals beschreven in paragraaf 3.2. Dit is gedaan door een download van de data uit Limesurvey te maken naar Excel waar vervolgens de controles zijn uitgevoerd. Eerst is een overzicht gemaakt van het aantal keer dat een antwoord per respondent gegeven is. De antwoorden zijn vertaald naar cijfers. Zo is "helemaal oneens"1, "oneens" 2 enzovoorts. De grote aantallen van gelijke antwoorden zijn bekeken. Er is gekeken of deze grote aantallen hebben geleid tot reeksen. Er zijn bij 2 respondenten reeksen gevonden van hetzelfde antwoord, niet overeenstemmende met de positieve of negatieve verwoording van de vragen. Deze zijn verwijderd. Daarnaast is gekeken naar patronen. Er is bij één respondent 3x een patroon ontdekt van de antwoordopties 5 en 1, ook niet overeenstemmend met de positieve en negatieve vraagstellingen, wat heeft geleid tot verwijdering.

Vervolgens is de data ingeladen in SPSS. Er zijn ISA scores bepaald op basis van de gegeven antwoorden op de manier zoals beschreven in paragraaf 3.2. Dit is apart gedaan voor ISA totaal, kennis, houding en gedrag. Er waren 4 respondenten die geen gebruik maken van een laptop. Deze scoorden bij een aantal vragen antwoord 6: "ik maak geen gebruik van een laptop." Antwoord 6 heeft hier niet de betekenis van een hoge ISA score en daarom is deze in de omzetting naar de schaal voor ISA leeg gelaten, omdat dit anders een vertekend beeld zou geven. Opleidingsniveau is her gecodeerd naar numerieke waarden, waarbij een hoger getal een hoger opleidingsniveau weergeeft. Basisonderwijs bleek in Limesurvey foutief gecodeerd. Dit is in SPSS omgezet van O1 naar 01.

4.2. Opleidingsniveau en ISA

In deze deelparagraaf wordt het resultaat beschreven van de toetsing of opleidingsniveau van invloed is op ISA of op de onderdelen van ISA. Dit wordt gedaan door toetsing van de volgende hypothesen (zie ook paragraaf 2.4):



Eerst worden de afzonderlijke variabelen bekeken en beschreven met kengetallen. Daarna wordt opleidingsniveau in aparte spreidingsdiagrammen uitgezet tegenover de score voor ISA, kennis, houding en gedrag. Ten slotte worden correlatieanalyses uitgevoerd voor de vier hypotheses.

Het opleidingsniveau van alle respondenten is uitgezet in een frequentietabel en in een staafdiagram (zie bijlage 8). De modale opleiding, de opleiding met de hoogste frequentie, is Bachelor HBO of WO. De mediaan is ook Bachelor HBO of WO, wat wil zeggen dat 50% van de respondenten een Bachelor HBO of WO heeft of hoger. Havo, MBO-niveau 4 is ook ruim vertegenwoordigd met 24%. Basisonderwijs, MBO-niveau 1 en Doctorsgraad komen maar één keer voor. De overige opleidingsniveaus komen minimaal 5 maal voor.

De scores van ISA en kennis, houding en gedrag zijn uiteengezet in histogrammen (bijlage 9) en een aantal kengetallen. Deze kengetallen zijn in onderstaande tabel naast elkaar weergegeven.

Kengetallen	ISA totaal	Kennis	Houding	Gedrag
N	355	355	355	355
Gemiddelde	4,25	4,27	4,30	4,18
Std.deviatie	0,39	0,42	0,40	0,43
Variantie	0,15	0,18	0,16	0,18
Minimum	3,24	2,95	3,14	3,24
Maximum	5	5	5	5

Tabel: kengetallen ISA totaal, kennis, houding en gedrag.

De gemiddelde scores verschillen niet veel van elkaar en vallen ruimschoots binnen de standaard deviatie. De maximale score is bij alle onderdelen 5. De minimale score is duidelijk het laagst bij kennis. In paragraaf 4.3 wordt nog apart bekeken of er variatie is vast te stellen tussen kennis, houding en gedrag. Er zijn 4 scores “missing.” Dit zijn de respondenten die geen gebruik maken van een laptop.

In spreidingsdiagrammen (bijlage 10) zijn alle scores van respectievelijk ISA, kennis, houding en gedrag van alle opleidingsniveaus geplot. In deze spreidingsdiagrammen is geen stijging in scores waar te nemen lopend van een laag opleidingsniveau naar een hoog opleidingsniveau, wat zou kunnen duiden op een positieve samenhang. Om de hypotheses te toetsen is vervolgens een

correlatieanalyse uitgevoerd om te kijken of er een positieve correlatie bestaat tussen opleidingsniveau enerzijds en ISA, kennis, houding en of gedrag anderzijds. Er wordt gekozen voor de correlatieanalyse, omdat het gaat om de samenhang tussen een kwantitatieve (ISA) en een ordinale (opleidingsniveau) variabele met veel verschillende meetwaarden van ISA en waarbij ook getracht wordt in beeld te brengen of het een positieve of negatieve samenhang is (Hacken ten, 2017). De uitkomst van de correlatieanalyse is Spearman's correlatiecoëfficiënt. Er is gekozen voor Spearman en niet voor Pearson omdat je hier niet over lineariteit spreekt. Immers zijn de opleidingen in klassen verdeeld van oplopend niveau en is de onderlinge afstand tussen de klassen niet meetbaar (Ramzai, 2020). Bij een positieve correlatie ligt deze waarde tussen 0-1. Daarnaast wordt gekeken of de waarde significant is. Dit is het geval als de Sig-waarde kleiner is dan 0,05. Anders gezegd, als Spearman's 'rho' significant van 0 afwijkt dan er is een positieve correlatie tussen de variabelen.

Correlatie Opleidingsniveau	ISA totaal	Kennis	Houding	Gedrag
Spearman's rho	0,044	0,042	0,078	-0,003
Sig. (1-tailed)	0,207	0,213	0,070	0,475
N	355	355	355	355

Tabel: correlatie opleidingsniveau en ISA totaal, kennis, houding en gedrag.

Spearman's correlatiecoëfficiënt geeft voor alle dimensies licht positieve waarden, behalve voor gedrag welke licht negatief is, maar ze wijken allemaal nauwelijks af van 0. Er kan niet gesproken worden van een significante correlatie aangezien de significantiewaarde steeds groter is dan 0.05. De hypothesen moeten dus worden verworpen. Er kan geen positieve correlatie vastgesteld worden tussen opleidingsniveau en ISA en ook niet tussen opleidingsniveau en kennis, houding of gedrag.

4.3. Variatie in ISA, kennis, houding of gedrag bij opleidingen

In deze deelparagraaf worden de onderzoeksresultaten beschreven van de toetsing of enig opleidingsniveau een hogere ISA heeft. Daarnaast of enig opleidingsniveau een hogere kennis, betere houding of beter gedrag heeft.

Om dit te kunnen bepalen wordt gebruik gemaakt van de variantieanalyse. Door middel van variantieanalyse wordt berekend of bij ISA totaal, of binnen één van de dimensies (kennis, houding of gedrag), een groep (opleidingsniveau) afwijkt van het gemiddelde. De variantieanalyse is geschikt omdat het gaat om een variabele die ordinaal is met een beperkt aantal meetwaarden en een variabele die kwantitatief is (Hacken ten, 2017). Voor alle vier de dimensies staan in bijlage 12 een frequentietabel en de kengetallen van de variantieanalyse zoals uitgevoerd. Uit de frequentietabellen blijkt, dat de verschillen tussen de gemiddelden van de diverse opleidingsniveaus klein zijn. Enige uitschieter is hier het gemiddelde van de groep Associate degree, dat duidelijk hoger is bij ISA totaal, kennis, houding en gedrag. Het aantal respondenten binnen deze groep is met 5 echter zo klein dat dit deze uitschieter veroorzaakt kan hebben en dus niet als relevant kan worden gezien. Gedrag heeft als dimensie duidelijk de laagste gemiddelde score. Bij gedrag valt verder het met afstand laagste gemiddelde van MBO-niveau 2 op. Aan de hand van de varianties kan worden nagegaan of de verschillen inderdaad zo klein zijn dat niet van een samenhang kan worden gesproken tussen opleidingsniveau en ISA of opleidingsniveau en de dimensies van ISA. Opleidingsniveau 1, 2 en 10 hebben geen standaard deviatie omdat het maar om 1 waarde gaat.

De variantieanalyse is uitgevoerd met de Anova toets en geeft als resultaat de waarden zoals hieronder in de tabel zijn weergegeven.

Anova	ISA totaal	ISA kennis	ISA houding	ISA gedrag
F	1,266	1,421	1,076	1,279
Sig.	0,254	0,178	0,380	0,247

Tabel: Anova.

Uit de Anova tabel blijkt dat de overschrijdingswaarde (Sig.) in alle gevallen ruim groter is dan 0,05. Dit betekent dat de gemiddelden niet significant van elkaar verschillen. De conclusie is daarom, dat geen enkel opleidingsniveau een significant hogere ISA heeft. Er is ook geen enkel opleidingsniveau wat een significant hogere kennis, betere houding of beter gedrag heeft.

4.4. IT-opleiding en ISA

In deze deelparagraaf worden de onderzoeksresultaten beschreven die betrekking hebben op de vraag of een IT-opleiding leidt tot een hogere ISA, een hogere kennis, betere houding of beter gedrag.

Hiertoe zijn twee groepen gevormd, respondenten met een IT-opleiding en respondenten zonder IT-opleiding. Deze groepen zijn in een cirkeldiagram en een frequentietabel uiteen gezet (bijlage 13). Van alle respondenten heeft 14,5% een IT-opleiding gevolgd en 85,5% niet. In onderstaande tabel staan de gemiddelde scores voor respondenten met een IT-opleiding en respondenten zonder IT-opleiding. Te zien is dat de gemiddelden voor respondenten met een IT-opleiding in alle dimensies hoger is.

	IT-opleiding	Gemiddelde	Std. Deviatie
ISA totaal	ja	4,480	0,317
	nee	4,211	0,388
ISA kennis	ja	4,506	0,314
	nee	4,231	0,423
ISA houding	ja	4,512	0,345
	nee	4,259	0,399
ISA gedrag	ja	4,423	0,366
	nee	4,144	0,423

Tabel: Gemiddelde en standaard deviatie IT-opleiding versus geen IT-opleiding.

Om te bepalen of dit verschil significant is wordt de ISA score van de twee groepen met elkaar vergeleken door middel van de T-toets. De T-toets wordt gebruikt omdat de variabele IT-opleiding dichotoom is, namelijk ja of nee, en de andere variabele kwantitatief (Hacken ten, 2017). Als de gemiddelde ISA voor beide groepen gelijk is, dan maakt het voor de hoogte van ISA niet uit of een werknemer een IT-opleiding heeft gevolgd of niet. Als de gemiddelden significant verschillen dan maakt het voor de hoogte van de ISA wel uit of iemand een IT-opleiding heeft gevolgd. De hypothese is dat het verschil van de gemiddelden positief is, ten gunste van respondenten met een IT-opleiding. De t-test bestaat uit twee delen. Levene's Test for Equality of Variances analyseert of de variantie van beide groepen IT en niet IT gelijk is. Dit bepaalt of je de t-waarde in de bovenste of onderste rij van de tabel moet aflezen (bijlage 13). Wanneer de significantie onder de 0.05 ligt, dan hebben we te maken met ongelijke varianties, daarboven met gelijke varianties. Hieronder een overzicht van de gevonden t-waarden en de bijbehorende significanties. Bij een significantiewaarde (Sig. 2-tailed)

kleiner dan 0.050 kun je concluderen dat er significante verschillen zijn in de gemiddelden van de twee groepen (Hacken ten, 2017)

	Levene's test	t-test for equalilty of means	
	Sig.	t	Sig. (2-tailed)
ISA totaal	0,080	4,694	0,000
ISA kennis	0,044	5,486	0,000
ISA houding	0,077	4,268	0,000
ISA gedrag	0,306	4,439	0,000

Tabel: Levene's test en t-test for equality of means.

We kunnen vaststellen dat de gemiddelde ISA score van respondenten met een IT-opleiding significant verschilt en wel hoger is dan van respondenten zonder IT-opleiding. Ook de scores voor kennis, houding en gedrag zijn significant hoger voor respondenten met een IT-opleiding.
De conclusie is:

- een IT-opleiding leidt tot een hogere ISA.
- een IT-opleiding leidt tot een hogere kennis van ISA.
- een IT-opleiding leidt tot een betere houding t.o.v. ISA.
- een IT-opleiding leidt tot een beter gedrag in het kader van ISA.

5. Discussie, conclusies en aanbevelingen

In dit hoofdstuk staan de discussie en conclusies naar aanleiding van het onderzoek en worden de onderzoeksvragen beantwoord. Tevens wordt aangegeven wat bedrijven naar aanleiding van dit onderzoek wel of juist niet zouden moeten doen met betrekking tot ISA en worden aanbevelingen gedaan voor verder wetenschappelijk onderzoek.

5.1. Discussie – reflectie

In deze paragraaf worden de conclusies uit het onderzoek bediscussieerd.

De belangrijkste conclusie uit dit onderzoek is, dat er geen positieve correlatie is tussen opleidingsniveau en ISA. Een hogere opleiding leidt dus niet tot een hogere ISA. Een hogere opleiding leidt ook niet tot hogere kennis, betere houding of beter gedrag. De theorie die ten grondslag ligt aan de opgestelde hypothesen wordt dus niet bevestigd. Deze theorie is, zoals in paragraaf 2.3 en 2.4 beschreven, gebaseerd op de bevindingen van Öğütçü et al. (2016) en Chua et al. (2018), dat er een significant effect bestaat van opleidingsniveau op ISA respectievelijk ISP awareness en tevens een significant effect van opleidingsniveau op nakoming van de regels c.q. gedrag. De resultaten sluiten echter meer aan bij het onderzoek van Pattinson et al. (2015), waarin geen positief verband kon worden vastgesteld tussen opleidingsniveau en Infosec gedrag. Er is geen directe verklaring voor het feit dat de hypotheses verworpen worden. Het kan te maken hebben met de specifieke caseorganisatie of het feit dat het een bedrijf is. Het onderzoek van Öğütçü et al. (2016) werd immers uitgevoerd bij studenten, academici en medewerkers van een universiteit. Het onderzoek van Chua et al. (2018) veronderstelt anderzijds dat er een Information Security Policy is en dat mensen met een hoger opleidingsniveau zich daarvan beter bewust zijn en deze ook beter naleven. Nu is tijdens het onderzoek gebleken dat de case organisatie niet over zo'n policy beschikt althans niet in een vorm die wordt uitgedragen in de organisatie. Het onderzoek heeft dus een meer algemene awareness gemeten en niet de kennis van een bestaande policy. In paragraaf 5.3 volgt een aanbeveling ten aanzien van dit onderwerp.

De volgende conclusie is dat er geen verschil is in de gemiddelde ISA bij verschillende opleidingsniveaus. Er is ook geen verschil in de gemiddelde kennis, de gemiddelde houding, of het gemiddelde gedrag bij verschillende opleidingsniveaus. Dit in tegenstelling tot de theorie van (Aydın & Chouseinoglou, 2013), die stellen dat gebruikers van information systems door hun verschillend beroep en verschillende opleidingsachtergrond een verschillend niveau van security awareness hebben. Het huidige onderzoek spreekt dat dus tegen. De case organisatie lijkt een groep gelijkgestemden die, ondanks of juist door het gebrek aan een Information Security Policy, op eenzelfde manier denken over security onderwerpen. Opvallend daarbij was de hoge response met 50% en Cronbach's alpha die met 0,954 voor de enquêtevragen erg hoog te noemen is. De uitkomst kan daarom heel specifiek zijn voor deze organisatie en dat dient verder onderzocht te worden door vergelijkingen met andere bedrijven.

Tenslotte kan geconcludeerd worden, dat een IT-opleiding leidt tot een hogere ISA, een hogere kennis, betere houding en beter gedrag. Dit is een toevoeging aan de bestaande kennis. Hoewel Kritzinger and Smith (2008) in hun onderzoek reeds spreken van verschillen in ISA voor professionals versus low-level users, waarbij medewerkers op professional level de benodigde kennis en ervaring hebben voor het omgaan met technical information security issues, spreken we bij dit onderzoek niet over technical users. Immers de echte technical users, namelijk de personen werkzaam op de afdeling IT security, waren uitgesloten van dit onderzoek. Een algemene IT opleiding blijkt dus ook tot een hogere ISA te leiden. Het zou interessant zijn om te onderzoeken of juist de recenter

afgestuurde IT'ers verantwoordelijk zijn voor deze hogere ISA. Bulgurcu et al. (2010) kwamen destijds immers tot de conclusie dat een hoger niveau van opleiding en kennis van technologie niet leidde tot een grotere intentie om te voldoen aan het Information security beleid. Intussen zou dit mogelijk veranderd kunnen zijn doordat bij IT-opleidingen meer aandacht voor security is. Of dit zo is zou verder onderzocht moeten worden.

De resultaten van het onderzoek mogen als valide beschouwd worden, omdat het instrument waarmee gemeten is, de HAIS-Q vragenlijst, een wetenschappelijk beproefde methode is om de ISA te meten van een populatie (Parsons et al., 2017). Het gebruik van het programma SPSS voor verwerking van de gegevens waarbij standaard statistische toetsen zijn gebruikt draagt ertoe bij dat herhaling relatief eenvoudig is, wat de betrouwbaarheid van het onderzoek ten goede komt. Indien het onderzoek op basis van de beschreven methode nogmaals wordt uitgevoerd zou dit moeten leiden tot dezelfde resultaten. Daarbij moet de opmerking worden gemaakt dat een meting een momentopname is en respondenten anders kunnen reageren op andere momenten. Hierna wordt beschreven in hoeverre er bij de uitvoering van het onderzoek afwijkingen zijn geweest van het oorspronkelijke plan en of deze van invloed zijn geweest op de betrouwbaarheid van de resultaten. Ook worden de beperkingen van de HAIS-Q methode besproken.

Het originele plan was om de enquête breed aan te kondigen via interne media bij de caseorganisatie. Van dit plan is afgeweken omdat er problemen waren met goedkeuring voor de enquête, waarbij bleek dat deze bij andere en meerdere personen verkregen moest worden. Medewerkers hebben daardoor voorafgaand aan de enquête niet van de directie te horen gekregen dat het onderzoek belangrijk is en dat men wordt verzocht om de vragenlijst in te vullen. Door uitblijvende goedkeuring is onder verantwoording van de CIO de enquête uiteindelijk uitgezet, waarbij directie en topmanagement werden uitgesloten van deelname. Omdat deze laatste groep slechts zo'n 20 personen betrof op een totale populatie van 746 zal dit aantal op zich niet veel invloed hebben gehad op de uitkomst van het onderzoek. Het belang van de enquête werd in het begeleidend schrijven wel benadrukt en vragen over de authenticiteit van de enquête werden persoonlijk beantwoord door de onderzoeker of de Securitymanager. In een ideale situatie zou men van het bedrijf zelf te horen moeten krijgen dat het onderzoek belangrijk is en dat men ruim de tijd krijgt, binnen werktijd, om de vragenlijst in te vullen. Ondanks dat is de response met 50% hoog te noemen, waardoor geconcludeerd mag worden dat de respondenten voldoende gemotiveerd waren om de vragenlijst in zijn geheel in te vullen. Het advies is om voorafgaand aan een enquête de volledige medewerking van de caseorganisatie goed te regelen bij de verantwoordelijke personen.

Tijdens het onderzoek is ervoor gekozen om onderzoek naar de invloed van een technische opleiding op ISA om te zetten naar de vraag of een IT-opleiding is gevolgd. Het vaststellen of een IT-opleiding is gevolgd is namelijk een Ja/Nee vraag. Er zijn veel verschillende technische opleidingen waarbij de mate van het technische aspect zeer varieert. De invloed ervan op ISA is dan niet helder en eenduidig vast te stellen.

Er is geen onderzoek gedaan naar de scores op focusgebieden zoals bijvoorbeeld wachtwoordgebruik, e-mailgebruik of internetgebruik bij verschillende opleidingsniveaus. Voor de volledigheid zou dit nog onderzocht kunnen worden.

In eerste instantie werd in hoofdstuk 3 beschreven dat er informatie nodig was over de hoogst genoten opleiding. Dit is uiteindelijk aangepast naar laatst genoten opleiding. Mensen met een lage opleiding zouden de vraag anders mogelijk als discriminerend op kunnen vatten. Ook zou worden gevraagd naar wat voor opleiding gevolgd is. Hiervoor is uiteindelijk niet gekozen. Dit heeft twee redenen. Het onderzoek gaat niet over een vergelijk tussen opleidingen t.a.v. ISA aspecten maar

over de invloed van het opleidingsniveau op ISA. Ten tweede is dit praktisch gezien erg lastig in te vullen en moet je je afvragen wat je daar statistisch gezien voor consequenties aan kunt verbinden. Dit zou namelijk een open vraag moeten worden voor de enquête omdat het ondoenlijk is om alle soorten opleidingen op te noemen. De invloed van bepaalde (voor-) opleidingen op ISA zou alsnog apart onderzocht kunnen worden.

Voor de caseorganisatie is apart buiten dit onderzoek om onderzoek gedaan naar verschillen tussen afdelingen. Het was namelijk interessant voor de caseorganisatie om te weten hoe afdelingen ten opzichte van elkaar scoren. Daarnaast kan het bedrijf de uitkomsten gebruiken in de aanpak voor de educatieve maatregelen. Bijvoorbeeld starten bij de laagst scorende afdeling op een bepaald onderdeel. Daarom is in de enquête een vraag toegevoegd op welke afdeling een respondent werkt. De groepen zijn dusdanig groot genomen dat anonimiteit gewaarborgd bleef.

Hierna worden een aantal beperkingen van de HAIS-Q vragenlijst besproken. Er kan niet beoordeeld worden of een antwoord op de enquête legitiem is, omdat antwoorden persoonlijk zijn en gaan over de kennis, houding en gedrag van die persoon. Het liefst zou je deze antwoorden controleren door feedback te vragen aan de respondent. Gezien de grootte van de groep en het feit dat de enquête anoniem is, is dit niet mogelijk. Het anonimiseren is juist gedaan om sociaal wenselijke antwoorden te voorkomen. Het niet kunnen verifiëren of bepaalde antwoorden bewust gegeven zijn is een nadeel van deze methode. Het liefst zou je alleen gemotiveerde respondenten hebben die zorgvuldig ieder antwoord kiezen en waarbij je dus zonder twijfel uit kunt gaan van de gekozen antwoorden. Dit is echter een utopie. Bij een online enquête zul je er toch rekening mee moeten houden dat je een bepaalde hoeveelheid “ruis” hebt. Omdat in dit geval het aantal respondenten behoorlijk groot was zullen een aantal afwijkingen niet van doorslaggevend belang zijn voor de uitkomst. Het is bij deze methode dan ook de bedoeling om een algemene indruk te krijgen van een fenomeen binnen een grote groep. Als de te onderzoeken populatie een stuk kleiner is zou je kunnen overwegen om de enquête persoonlijk, steekproefsgewijs af te nemen bij een beperkt aantal respondenten. Natuurlijk moet de steekproef dan wel voldoende groot zijn om uiteindelijk een uitspraak over de hele populatie te kunnen doen. Parsons et al. (2014) spraken in hun onderzoek over een “willekeurige vaste volgorde” van de enquêtevragen. Welke volgorde dat is wordt in hun onderzoek niet duidelijk. De manier waarop zij de vragen presenteren is in ieder geval dusdanig dat de vragen per aandachtsgebied, zoals wachtwoordbeheer of e-mailgebruik, achtereenvolgens gesteld worden. In het huidige onderzoek is ervoor gekozen om alle vragen daadwerkelijk in een willekeurige volgorde te stellen en daarbij ook de vragen over de aandachtsgebieden af te wisselen. Het negatief verwoorden van een aantal vragen en de random volgorde zouden juist de respondent ertoe aan moeten zetten om telkens opnieuw na te moeten denken over het antwoord. Het is de vraag of dit effect steeds wordt bereikt. Concentratiegebrek door het grote aantal vragen en of het niet goed lezen dan wel het niet begrijpen van de vraagstelling kan er juist voor zorgen dat dit averechts werkt. Tijdens het controleren van de data kom je namelijk antwoorden tegen waarbij je je afvraagt of deze zo bedoeld zijn of dat er sprake is van niet goed begrijpen van de vraag of haastig of ongeïnteresseerd invullen. Mogelijk had het toevoegen van extra instructies op dit gebied een positieve bijdrage kunnen leveren. Zoals expliciet vermelden in de instructie voorafgaand aan het invullen, dat onderwerpen worden afgewisseld en dat negatieve en positieve vraagstellingen door elkaar worden gebruikt.

Tenslotte een opmerking over de keuze voor de onderzoeksstrategie. De strategie was hier de case study maar een survey was in theorie ook een mogelijkheid geweest, waarbij onderzoek zou worden gehouden onder een groot aantal mensen bij diverse bedrijven. Hoewel de wetenschappelijke relevantie van een survey groter zou zijn geweest, was het in het kader van dit afstudeertraject niet

haalbaar om zo'n groot onderzoek te doen. Je hebt daarnaast voldoende organisaties nodig en bovendien toestemming om respondenten van die bedrijven te benaderen. Een longitudinaal onderzoek was ook interessant geweest waarbij over tijd nogmaals hetzelfde onderzoek wordt gedaan om te kijken wat dan het resultaat is. Ook dit was binnen de gegeven tijd niet haalbaar. Zeker indien in de tussentijd door de case organisatie door middel van educatie aandacht aan ISA zou zijn geschonken, was het interessant geweest om daarvan het resultaat vast te stellen in het tweede onderzoek.

5.2. Conclusies

In deze paragraaf staan de conclusies naar aanleiding van de onderzoeksresultaten.

Organisaties zoeken al jaren naar manieren om de ISA van hun medewerkers te verhogen. Door onderzoek zijn inmiddels diverse factoren bekend die van invloed zijn op ISA. Organisaties kunnen deze factoren gebruiken voor de invulling van organisatorische en educatieve maatregelen, om de ISA van hun medewerkers te vergroten en daarmee Infosec risico's te verlagen. De vraag is of opleidingsniveau één van de factoren is, die van invloed is op ISA.

Naar aanleiding van bevindingen uit eerder onderzoek zijn een aantal hypothesen opgesteld:

- er is een verband tussen opleidingsniveau en ISA
- er is een verband is tussen opleidingsniveau en kennis van ISA
- er is een verband is tussen opleidingsniveau en houding t.o.v. ISA
- er is een verband is tussen opleidingsniveau en gedrag in het kader van ISA

Alle hypothesen hierboven worden naar aanleiding van dit onderzoek verworpen. Het antwoord op de subvragen van het onderzoek luidt, dat medewerkers met een hogere opleiding de regels niet beter of slechter kennen dan mensen met een lagere opleiding. Ook met betrekking tot houding en gedrag is er geen verschil vast te stellen tussen medewerkers met een hogere of lagere opleiding. Specifiek is onderzocht of een IT-opleiding leidt tot een hogere ISA. Deze stelling wordt door het onderzoek bevestigd. Een IT-opleiding leidt ook tot betere kennis, een betere houding en beter gedrag.

5.3. Aanbevelingen voor de praktijk

In deze paragraaf wordt beschreven wat bedrijven wel of niet zouden moeten doen naar aanleiding van de onderzoeksresultaten en conclusies, met betrekking tot de ISA van medewerkers.

Het is aan te raden om medewerkers van bedrijven een security-training te geven om het kennisniveau van ISA op een hoger peil te krijgen. Eerder onderzoek zoals dat van McCormac, Zwaans, et al. (2017) bevestigt dat Infosecurity opleiding of training van invloed kan zijn op de ISA van medewerkers. Een dergelijk security education, training and awareness (SETA) programma, moet specifiek zijn voor de organisatie en, om effectief te zijn, niet alleen gericht zijn op de verhoging van de kennis maar ook op het verbeteren van de houding en het gedrag van de medewerkers (Alshaikh, Maynard, & Ahmad, 2021).

Bedrijven wordt in ieder geval aangeraden om een Information Security Policy te maken en deze ook uit te dragen. Daarnaast om regelmatig te toetsen hoe het gesteld is met de kennis van deze policy onder de medewerkers. Het hebben van kennis van de regels van Information Security zou namelijk ook leiden tot een betere houding en gedrag en aanzien van deze regels volgens het onderzoek van Parsons et al. (2014).

Een vervolgonderzoek bij hetzelfde bedrijf zou interessant zijn om over enige tijd vast te stellen of, nog te nemen, educatieve maatregelen hun effect hebben gehad.

5.4. Aanbevelingen voor verder onderzoek

In deze paragraaf wordt beschreven welke aanbevelingen er worden gedaan voor verder wetenschappelijk onderzoek naar aanleiding van de resultaten en conclusies van dit onderzoek.

Aangezien het onderzoek niet heeft kunnen bevestigen dat er een positieve correlatie bestaat tussen opleidingsniveau en ISA maar omdat andere onderzoeken dit wel vermoeden, is het aan te raden om hier verder onderzoek naar te doen. De beperkingen van dit onderzoek zijn met name dat de uitkomsten alleen iets zeggen over deze specifieke case. Een vervolgonderzoek bij andere bedrijven wordt daarom aanbevolen om zo meer data te verzamelen en te kunnen vergelijken. Dit kan zijn in dezelfde sector, om verschillen tussen bedrijven in dezelfde sector te onderzoeken. Of juist in verschillende sectoren om vast te stellen of er verschillen zijn tussen verschillende sectoren.

Er is niet onderzocht of er verschil is in de gemiddelde scores per opleiding op de diverse aspecten zoals e-mail, wachtwoordgebruik en dergelijke. Dit zou nog verder onderzocht kunnen worden eventueel met gebruik van dezelfde data. Herhaling van hetzelfde onderzoek, een longitudinaal onderzoek, is ook een mogelijkheid waarbij niet onderzochte aspecten dan direct worden meegenomen.

Het onderzoek bevestigt dat een IT-opleiding een significant positief effect heeft op ISA. Het zou interessant zijn om te onderzoeken of juist de recenter afgestuurde IT’ers verantwoordelijk zijn voor deze hogere ISA. In het verleden leidde een hoger niveau van opleiding en kennis van technologie namelijk niet tot een grotere intentie om te voldoen aan het Information security beleid (Bulgurcu et al., 2010).

Referenties

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security, 100*, 102090. doi:https://doi.org/10.1016/j.cose.2020.102090

Aydın, Ö. M., & Chouseinoglou, O. (2013). Fuzzy Assessment of Health Information System Users' Security Awareness. *Journal of Medical Systems, 37*(6), 1-13. doi:10.1007/s10916-013-9984-x

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

Coopers, P. (2013). Key findings from the Global State of Information Security Survey 2013. *Changing the game*.

Hacken ten, P. (2017). SPSS handleiding bij de cursus: Methoden en technieken van onderzoek (Premaster). In: Open Universiteit; Opleiding Managementwetenschappen.

Kiss, G. (2019). The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education. *SHS Web of Conferences, 66*, 1042. doi:10.1051/shsconf/20196601042

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5-6), 224-231.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses. *Australasian Journal of Information Systems, 21*. doi:10.3127/ajis.v21i0.1697

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151-156. doi:10.1016/j.chb.2016.11.065

McIlwraith, A. (2016). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*: Gower.

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological methods, 17*(3), 437.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. doi:10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi:10.1016/j.cose.2013.12.003

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). *Factors that Influence Information Security Behavior: An Australian Web-Based Study*, Cham.

Ramzai, J. (2020, June 25). Clearly explained: Pearson versus Spearman Correlation Coefficient. Retrieved from https://towardsdatascience.com/clearly-explained-pearson-v-s-spearman-correlation-coefficient-ada2f473b8

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Harlow: Pearson.

Šolić, K., Pleša, M., Velki, T., & Nenadić, K. (2019). Awareness About Information Security And Privacy Among Healthcare Employees. *3*(1), 21-28. doi:10.26332/seemedj.v3i1.88

Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. *AMCIS 2004 proceedings*, 175.

Tsohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People, 31*(5), 1047-1068. doi:10.1108/ITP-02-2017-0052

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*, 101640. doi:10.1016/j.cose.2019.101640

Bijlage 1 Bepaling en uitvoering query's

Omdat het onderzoek gaat over Information security awareness, wordt in eerste instantie naar een exacte match hiervan in de titel gezocht.
Query 1:

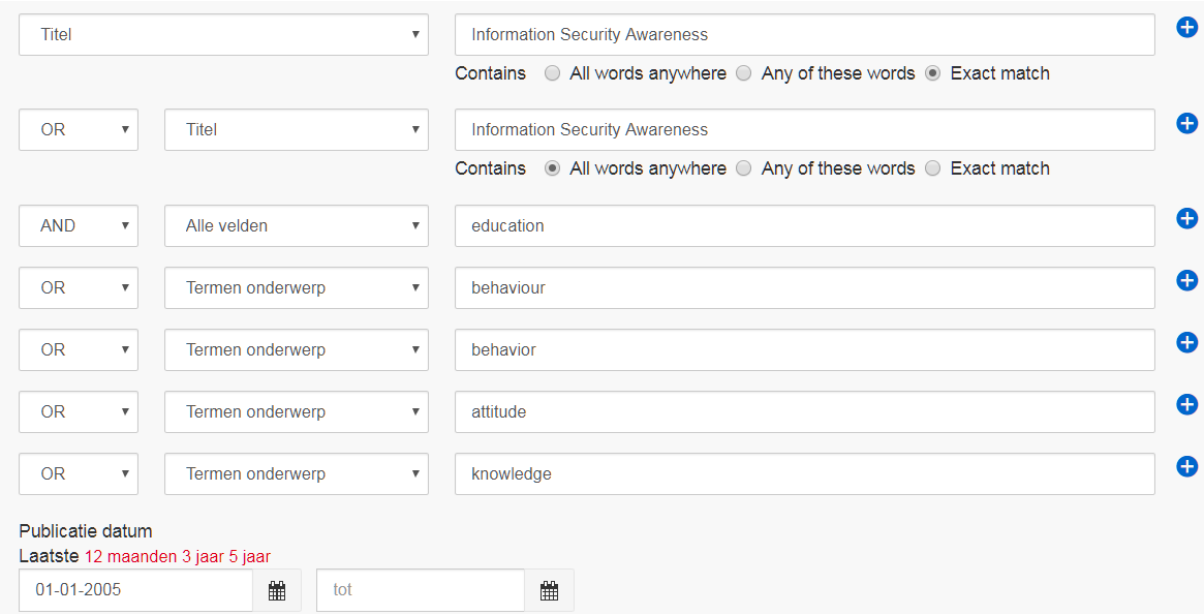
- Information Security Awareness; exact in de titel

Om de kans op bruikbare resultaten te vergroten, wordt vervolgens wederom naar de woorden Information security awareness gezocht in de titel maar met de woorden op een willekeurige plaats. Dit wordt gecombineerd met query 1, om de resultaten daarvan in ieder geval te behouden.
Query 2:

- Information Security Awareness; exact in de titel
- OR Information Security Awareness; anywhere in de titel

Deze resultaten worden verfijnd c.q. verder toegespitst op het onderzoek, door in de gehele tekst te zoeken naar het woord education, omdat education in relatie tot ISA een grote rol speelt in het onderzoek. Education zou tenminste in de tekst van de literatuur voor moeten komen. Als education niet in de tekst voor komt, dient tenminste één van de woorden kennis, houding of gedrag uit de onderzoeksvragen in de onderwerpen van de literatuur voor te komen. Van gedrag blijken twee Engelse woorden in omloop, behaviour en behavior. Daarom worden deze allebei gebruikt. Deze instellingen worden samen verwerkt in query 3. De exacte instellingen zijn te zien in bijlage 1.
Query 3:

- Information Security Awareness; exact in de titel
- OR Information Security Awareness behavior; anywhere in de titel
- AND eduation in alle velden
- OR behaviour in termen onderwerp
- OR behavior in termen onderwerp
- OR attitude in termen onderwerp
- OR knowledge in termen onderwerp



Query nummer 3: De zoekmachine interpreteert dit als: (a of b) en (c of d of e of f of g).

De resultaten van de derde query worden gesorteerd op datum, waarna de 25 meest recente resultaten allemaal worden bekeken. Mocht dit, inclusief referenties en citatie-analyse, niet voldoende bronnen opleveren, dan worden de eerst volgende 5 resultaten bekeken enzovoorts.

Na het lezen van de geselecteerde artikelen moet blijken of deze inderdaad geschikt zijn om te gebruiken of niet. Dit is afhankelijk van het feit of er aanwijzingen in staan die gebruikt kunnen worden als bron voor de beantwoording van de onderzoeksvragen. Dit kunnen bijvoorbeeld stellingen zijn, die ISA in verband brengen met opleiding, kennis, houding of gedrag. De artikelen die hiervoor geselecteerd worden, vormen samen het aantal relevante artikelen.

Als bron kan ook literatuur worden aangevoerd, die in de literatuurlijst voor komt van een van de relevante bronnen. Deze literatuur wordt geselecteerd om te lezen, indien voor het onderzoek interessante stellingen worden aangehaald uit die literatuur. Stellingen die verband houden met de onderzoeksvragen.

Ook wordt gekeken of relevante literatuur wordt geciteerd in andere onderzoeken. Deze citatie-analyse wordt alleen gedaan bij relevante literatuur waarin een nadrukkelijk en positief verband wordt beschreven tussen opleidingsniveau en ISA of onderdelen van ISA, want dan kunnen mogelijk vervolgonderzoeken gevonden worden op hetzelfde thema die bruikbaar zijn. Bij citatie-analyse wordt literatuur geselecteerd om in zijn geheel te lezen op basis van titel, samenvatting en onderwerpen. Deze moeten verband houden met de onderzoeksvragen van het onderzoek. Uiteraard geldt voor uiteindelijke selectie hetzelfde, dat er aanwijzingen in die literatuur dient te staan die gebruikt kan worden als bron voor de beantwoording van de onderzoeksvragen. Hoeveel literatuur vanuit referenties is toegevoegd of door middel van citatie-analyse, wordt in paragraaf 2.2 toegelicht.

De query's worden achtereenvolgens uitgevoerd, waarbij het aantal resultaten is vastgelegd. De 32 resultaten van query 1 worden niet bekeken maar de query wordt direct uitgebreid met een tweede zoekterm. Dit resulteert in query 2. Deze query levert 59 resultaten op. Dit is teveel om allemaal te bekijken en waarschijnlijk zijn ook niet alle resultaten bruikbaar. Daarom worden filters toegevoegd aan de query, om de resultaten meer toe te spitsen op de onderzoeksvragen. Deze derde query levert 39 resultaten op. Besloten wordt om met de 25 meest recente resultaten verder te gaan. Deze worden allemaal bekeken en hiervan blijken er 7 relevant. In 3 van de relevante resultaten staan in totaal 7 interessante verwijzingen naar andere literatuur. Deze 7 resultaten zijn allemaal bekeken en daarvan blijken er 4 relevant te zijn. Het totaal aantal relevante resultaten komt daarmee op 11. Als laatste is citatie-analyse toegepast op 2 artikelen, zoals omschreven in de vorige alinea. Dit levert nog 4 artikelen op die bekeken zijn. Daarvan blijken er geen relevant. Voor 2 van deze artikelen was alleen een samenvatting beschikbaar. Welke dat zijn staat in bijlage 2. Het totaal aantal relevante resultaten blijft hierdoor 11.

Bijlage 2 Resultaten van de query's

Nr.	Titel	schrijver	jaartal	bekeken	relevant	literatuur lijst analyse	citatie analyse
1	Individual differences and Information Security Awareness	McCormac, A., Zwaans, T., Parsons, K., Calic,	2017	ja	ja	ja	nee
2	Analysis of personal information security behavior and awareness	Gizem Öğütçü	2016	ja	ja	nee	ja
3	Building an awareness-centered information security policy compliance model	Koohang	2019	ja	nee	nee	nee
4	More than the individual: Examining the relationship between culture and Information Security Awareness	Wiley	2019	ja	ja	ja	nee
5	Awareness About Information Security And Privacy Among Healthcare Employees	Solic	2019	ja	ja	nee	nee
6	A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness	Kam	2019	ja	nee	nee	nee
7	Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective	Park	2019	ja	nee	nee	nee
8	Exploring the role of work identity and work locus of control in information security awareness	Hadlington	2019	ja	nee	nee	nee
9	The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education	Kiss Gabor	2019	ja	ja	nee	nee
10	Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations	Chua, Hui Na; Wong, Siew Fan; Low, Yeh Chir	2018	ja	ja	nee	ja
11	The impact of information security threat awareness on privacy-protective behaviors	Mamonov	2018	ja	nee	nee	nee
12	Persona-centred information security awareness	Ki-Aries, Duncan; Faily, Shamal	2017	ja	nee	nee	nee
13	From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance	Bauer	2017	ja	nee	nee	nee
14	Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security	Bauer	2017	ja	nee	nee	nee
15	Shaping intention to resist social engineering through transformational leadership, information security culture	Flores	2016	ja	nee	nee	nee
16	Providing Information on the Spot: Using Augmented Reality for Situational Awareness in the Security Domain	Lukosch	2015	ja	nee	nee	nee
17	Explore Awareness of Information Security: Insights from Cognitive Neuromechanism	Han	2015	ja	nee	nee	nee
18	A study on strengthening security_awareness_programs based on an RFID access control system for inside information	Choi	2015	ja	nee	nee	nee
19	Information disclosure of social media users Does control over personal information, user awareness and security notices	Benson	2015	ja	nee	nee	nee
20	Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs	Aggeliki Tsohou	2015	ja	nee	nee	nee
21	Developing a secured social networking site using informatio	Okesola	2014	ja	nee	nee	nee
22	Information security awareness and behavior: a theory-based literature review	Lebek, Benedict	2014	ja	nee	nee	nee
23	An exploratory investigation of message-person congruence	Kajzer	2014	ja	nee	nee	nee
24	Fuzzy Assessment of Health Information System Users' Secur	Aydin	2013	ja	ja	ja	nee
25	Information_Security_Awareness_Status of Business College:	Kim	2013	ja	nee	nee	nee
Via literatuurlijst van bron 1							
1	Factors that Influence Information Security Behavior	Malcolm Pattinson	2015	ja	ja		
2	Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)	Parsons, Kathryn. McCormac, Agata; Butavici	2014	ja	ja		
Via literatuurlijst van bron 4							
3	The effect of resilience and job stress on information security awareness	Mc.Cormac	2018	ja	nee		
4	Assessing information security attitudes: a comparison of two studies	Pattinson	2016	ja	nee		
5	Personality and it security: an application of the five-factor model	Shrobshire	2006	ja	nee		
Via literatuurlijst van bron 24							
6	Behavioral information security: two end user survey studies of motivation and security practices.	Stanton	2004	ja	ja		
In diverse gelezen stukken:							
7	Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness	Bulgurcu	2010	ja	ja		
Via citatieanalyse van bron 2							
1	The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory	Guhr	2018	ja; geheel	nee		
Via citatieanalyse van bron 10							
2	Building competitive advantage from Ubuntu: An African information security awareness model	Gundu	2020	ja; samenvatting	nee		
3	Lessons Learned from an Organizational Information Security Awareness Campaign	Scrimgeour	2019	ja; geheel	nee		
4	Antecedents of information security activities: Drivers, enablers, and constraints	Gallagher	2019	ja; samenvatting	nee		

Bijlage 3 Stellingen n.a.v. het literatuuronderzoek

Het literatuuronderzoek levert de volgende stellingen op:

- Geen significante invloed van opleidingsniveau op navolging ISP (Bulgurcu et al., 2010)
- Geen verband gevonden tussen opleidingsniveau en Infosec gedrag (Pattinson et al., 2015)
- Geen significant verschil in ISA aan het begin en eind van een studie (Kiss, 2019)
- Opleiding kan invloed hebben op ISA (McCormac, Zwaans, et al., 2017)
- Studies tonen aan dat hogere ISA in verband wordt gebracht met hogere opleiding (Wiley et al., 2020)
- verschillende opleidingen hebben verschillende mate van security awareness (Aydın & Chouseinoglou, 2013)
- Kennis van procedures heeft positieve invloed op houding en gedrag (Parsons et al., 2014)
- Er is een relatie tussen ISA en opleidingsniveau (Öğütçü et al., 2016)
- ISA en gedrag zijn nauw verbonden met elkaar (Öğütçü et al., 2016)
- Opleidingsniveau in Infosec verlaagt het risiconiveau in het gedrag (Öğütçü et al., 2016)
- opleidingsniveau heeft significant effect op ISP awareness (Chua et al., 2018)
- opleidingsniveau heeft significant effect op nakoming van de regels (Chua et al., 2018)
- hogere inkomens vertonen beter gedrag m.b.t. ISA (Stanton et al., 2004)
- hoger opgeleiden hebben een hoger risico ontwijkende houding (Aydın & Chouseinoglou, 2013)
- lager opgeleiden hebben een bewustere houding m.b.t bepaalde Infosec onderwerpen (Šolić et al., 2019)

Bijlage 4 HAIS-Q vragenlijst

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues. *
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. *
Considering consequences	I can't be fired for something I post on social media. *	It doesn't matter if I post things on social media that I wouldn't normally say in public. ^	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media. ^	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media. ^
Focus area: Mobile devices			
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. ^	When working in a public place, I leave my laptop unattended. ^
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. ^	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. *
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.*	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. ^	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. *	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. ^	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. ^
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. ^	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. ^	If I noticed my colleague ignoring security rules, I wouldn't take any action. ^
Reporting all incidents	It's optional to report security incidents. ^	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.

Note. Participants are instructed to respond to each item on a five-point scale from "Strongly Disagree" to "Strongly Agree".

Bijlage 5 HAIS-Q vragenlijst vertaald in het Nederlands

Vragen gaan over: (1) kennis van de richtlijnen van computer gebruik, (2) houding tegenover deze richtlijnen, (3) gedrag bij het gebruik van een computer voor het werk.

1. Kennis: “De volgende uitspraken gaan over uw kennis van hoe u een computer voor het werk moet gebruiken.”

Het is acceptabel om mijn social media wachtwoord te gebruiken voor mijn werk account.
Het is toegestaan om mijn werkwachtwoord te delen met mijn collega's.
Een mix van letters, cijfers en symbolen is noodzakelijk voor werkwachtwoorden.
Ik mag klikken op iedere link in e-mails van mensen die ik ken.
Ik mag niet klikken op een link in een e-mail van een onbekende afzender.
Ik mag bijlagen openen in e-mails van onbekende afzenders.
Ik mag ieder bestand downloaden op mijn werkcomputer, als dit mij helpt om mijn werk te doen.
Als ik aan het werk ben, zou ik bepaalde websites niet moeten bezoeken.
Ik mag op iedere website iedere informatie invoeren, als dit mij helpt om mijn werk te doen.
Ik moet periodiek de privacy instellingen van mijn social media accounts beoordelen.
Ik kan niet ontslagen worden voor iets wat ik plaats op social media.
Ik kan plaatsen wat ik wil over mijn werk op social media.
Als ik in een openbare ruimte aan het werk ben, moet ik mijn laptop altijd bij me houden.
Ik mag gevoelige werkbestanden versturen via een publiek Wi-Fi netwerk.
Als ik aan een gevoelig document werk, moet ik er zeker van zijn dat vreemden mijn scherm niet kunnen zien.
Afdrukken met gevoelige informatie kunnen op dezelfde manier worden weggegooid als niet gevoelige afdrukken.
Als ik een USB stick in een publieke ruimte vind, zou ik deze niet in mijn werkcomputer moeten stoppen.
Ik mag afdrukken die gevoelige informatie bevatten, 's nachts op mijn bureau laten liggen.
Als ik iemand zie die zich verdacht gedraagt in mijn werkomgeving, zou ik dit moeten rapporteren.
Ik moet slecht security gedrag van mijn collega's niet negeren.
Het is niet verplicht om security incidenten te melden.

2. Houding: “De volgende uitspraken gaan over uw houding. U heeft ons verteld over uw kennis van de richtlijnen voor computergebruik. Vertel ons nu wat u van deze richtlijnen vindt.”

Het is veilig om hetzelfde wachtwoord te gebruiken voor social media en werk accounts.
Het is een slecht idee om mijn werkwachtwoord te delen, zelfs als mijn collega's erom vragen.
Het is veilig om een werkwachtwoord te hebben wat alleen uit letters bestaat.
Het is altijd veilig om op links in e-mails te klikken van mensen die ik ken.
Er kan niks ernstigs gebeuren, als ik klik op een link in een e-mail van een onbekende afzender.
Het is riskant om bijlagen te openen in e-mails van onbekende afzenders.
Het kan riskant zijn om bestanden te downloaden op mijn werkcomputer.
Als ik een website kan bezoeken op het werk, betekent dit nog niet dat deze veilig is.
Als het mij helpt om mijn werk te doen, maakt het niet uit welke informatie ik plaats op een website.
Het is een goed idee om regelmatig de privacy instellingen van mijn social media accounts te beoordelen.
Het maakt niet uit als ik op social media dingen plaats, die ik in het openbaar normaal niet zou zeggen.
Het is riskant om bepaalde informatie over mijn werk te plaatsen op social media.
Als ik in een café aan het werk ben, is het veilig om mijn laptop 1 minuut onbeheerd achter te laten.

Het is riskant om gevoelige werkbestanden te versturen over een publiek Wi-Fi netwerk.
Het is riskant om gevoelige documenten te openen, terwijl vreemden mijn scherm kunnen zien.
Weggooien van afdrukken met gevoelige informatie in een vuilnisbak is veilig.
Als ik een USB stick in een publieke ruimte vind, kan er niets ernstigs gebeuren als ik deze in mijn werkcomputer stop.
Het is riskant om afdrukken die gevoelige informatie bevatten, 's nachts op mijn bureau te laten liggen.
Als ik iemand negeer die zich verdacht gedraagt in mijn werkomgeving, kan er niets ernstigs gebeuren.
Er kan niets ernstigs gebeuren, als ik slecht security gedrag van een collega negeer.
Het is riskant om security incidenten te negeren, ook al denk ik dat ze niet van belang zijn.

3. Gedrag: “De volgende uitspraken gaan over uw gedrag. U heeft ons verteld wat u weet en wat u denkt over richtlijnen over computergebruik. Vertel ons nu wat u doet als u een computer voor het werk gebruikt.”

Ik gebruik een ander wachtwoord voor mijn social media dan voor mijn werk account.
Ik deel mijn werkwachtwoord met collega's.
Ik gebruik een combinatie van letters, cijfers en symbolen in mijn werkwachtwoord.
Ik klik niet altijd op links in e-mails, ook al zijn ze afkomstig van iemand die ik ken.
Als een e-mail van een onbekende afzender er interessant uit ziet, klik ik op de link in die e-mail.
Ik open geen bijlagen in e-mails als ik de afzender niet ken.
Ik download ieder bestand op mijn werkcomputer, dat mij helpt om de klus te klaren.
Als ik op het werk op het internet ga, bezoek ik iedere website die ik wil.
Ik beoordeel de veiligheid van een website voordat ik informatie invoer.
Ik beoordeel niet regelmatig de privacy instellingen van mijn social media accounts.
Ik plaats geen dingen op social media, zonder vooraf de negatieve gevolgen te overwegen.
Ik plaats wat ik maar wil over mijn werk op social media.
Als ik in een openbare ruimte aan het werk ben, laat ik mijn laptop onbeheerd achter.
Ik verstuur gevoelige werkbestanden via een publiek Wi-Fi netwerk.
Ik controleer dat vreemden mijn scherm niet kunnen zien, als ik aan een gevoelig document werk.
Als afdrukken met gevoelige informatie weggegooid moeten worden, zorg ik ervoor dat ze in de shredder gaan of vernietigd worden.
Ik zou een USB stick, die ik in een publieke ruimte vind, niet in mijn werkcomputer stoppen.
Ik laat afdrukken die gevoelige informatie bevatten, op mijn bureau liggen als ik er niet ben.
Als ik iemand zie die zich verdacht gedraagt in mijn werkomgeving, zou ik er iets aan doen.
Als ik opmerk, dat een collega security regels negeert, zou ik geen actie ondernemen.
Als ik een security incident opmerk, zou ik het melden.

Bijlage 6 Populatie case organisatie

Rijlabels	Aantal van Personeelsnummer
BS Sales FS NL	395
HK Algemene zaken	20
HK BS Operations	9
HK Facilities	35
HK Financiën	51
HK Inkoop & Assortimentmgmt	71
HK IT	180
HK Kwaliteitscontrole	6
HK OBIB	19
HK Personeel & Organisatie	33
HK Programma & Procesmgmt	21
HK Supply Chain	53
HK Supply Chain Management	3
HK Uitzonderlijk personeel	9
Marketing FS NL	31
Overhead Foodservice NL	4
ZB FS NL	43
(leeg)	
Eindtotaal	**983**

Bijlage 7: Indeling Nederlands kwalificatieraamwerk (NLQF)

- ○ Basisonderwijs
- ○ VMBO, MBO-niveau 1 entreeopleiding
- ○ VMBO, MBO-niveau 2 beroepsopleiding
- ○ MBO-niveau 3 vakopleiding
- ○ HAVO, MBO-niveau 4 middenkader- of specialistenopleiding
- ○ VWO
- ○ Associate degree
- ○ Bachelor (HBO of WO)
- ○ Master (HBO of WO)
- ○ Doctorsgraad

Bijlage 8: Frequentietabel en staafgrafiek opleidingsniveau

Statistics

Opleidingsniveau

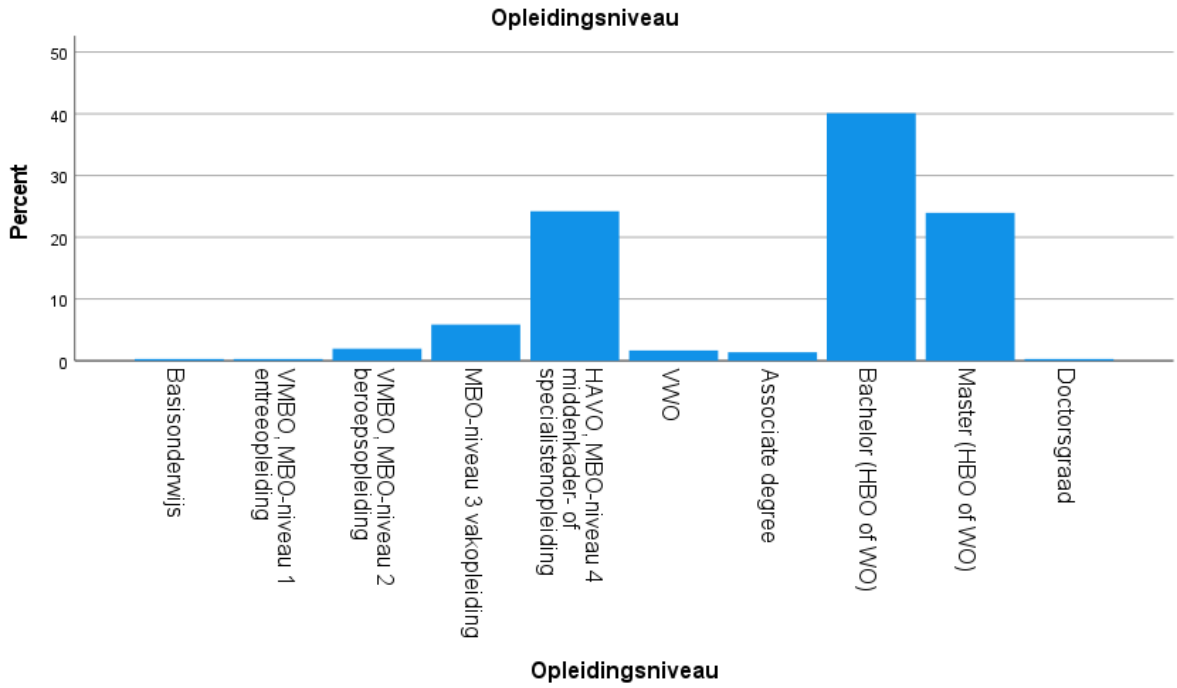
N	Valid	359
	Missing	0
Median		8,00
Mode		8

Tabel: mediaan en modus van opleidingsniveau

Opleidingsniveau

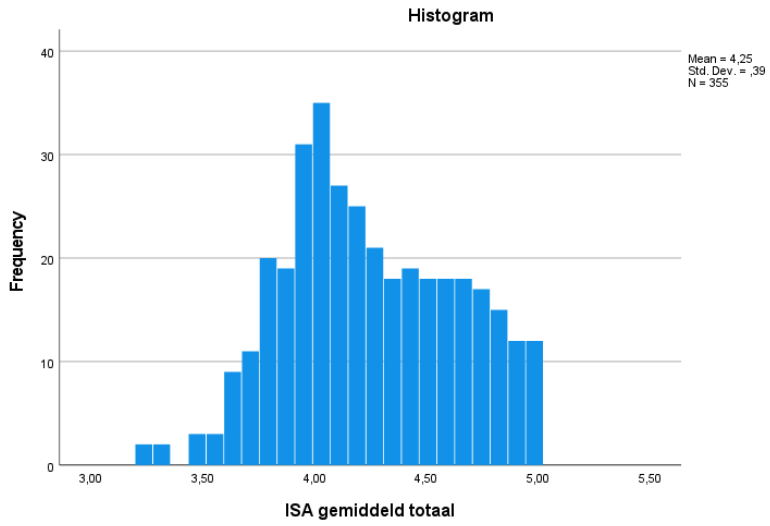
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Basisonderwijs	1	,3	,3	,3
	VMBO, MBO-niveau 1 entreeopleiding	1	,3	,3	,6
	VMBO, MBO-niveau 2 beroepsopleiding	7	1,9	1,9	2,5
	MBO-niveau 3 vakopleiding	21	5,8	5,8	8,4
	HAVO, MBO-niveau 4 middenkader- of specialistenopleiding	87	24,2	24,2	32,6
	VWO	6	1,7	1,7	34,3
	Associate degree	5	1,4	1,4	35,7
	Bachelor (HBO of WO)	144	40,1	40,1	75,8
	Master (HBO of WO)	86	24,0	24,0	99,7
	Doctorsgraad	1	,3	,3	100,0
	Total	359	100,0	100,0	

Frequentietabel: aantal en percentage respondenten per opleidingsniveau

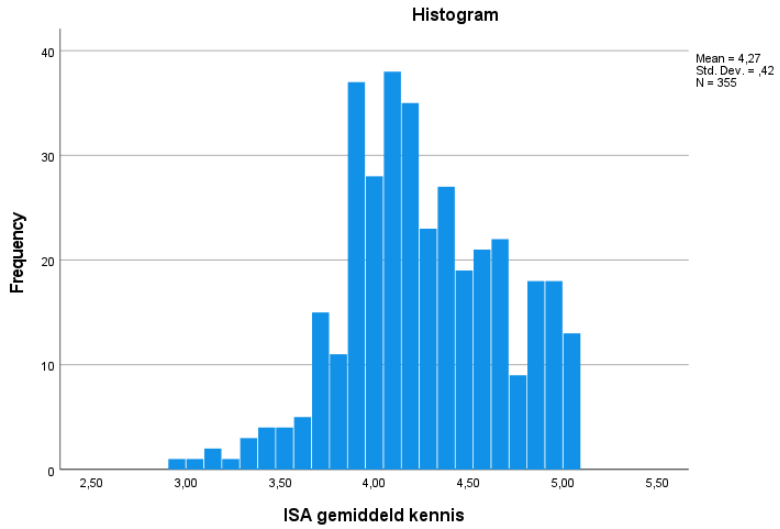


Staafgrafiek: percentage respondenten per opleidingsniveau

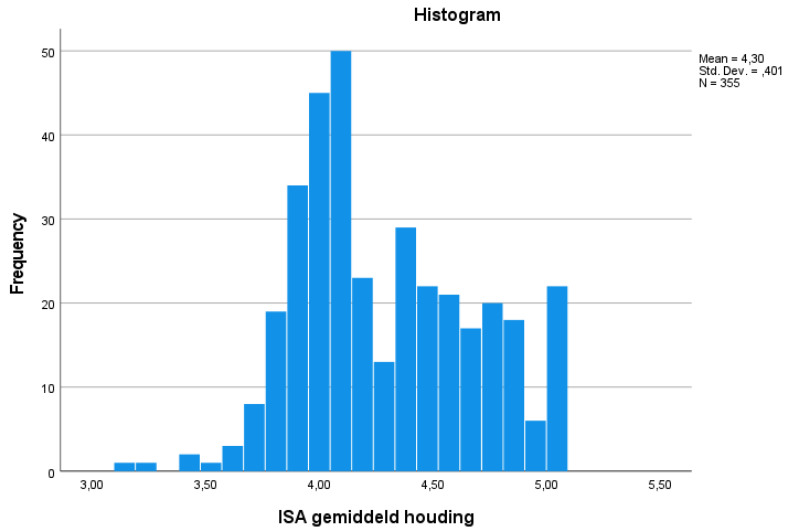
Bijlage 9: Histogrammen ISA totaal, kennis, houding en gedrag



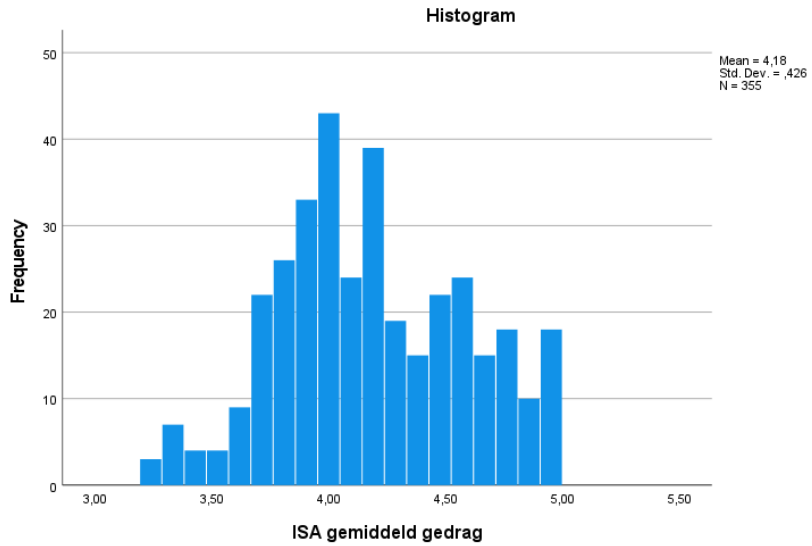
Histogram: frequentie van ISA gemiddeld totaal



Histogram: frequentie van ISA gemiddeld kennis

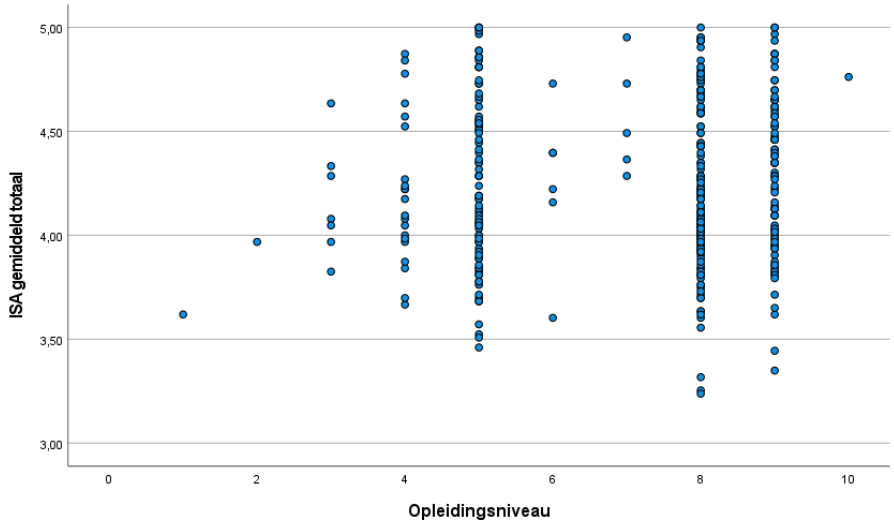


Histogram: frequentie van ISA gemiddeld houding

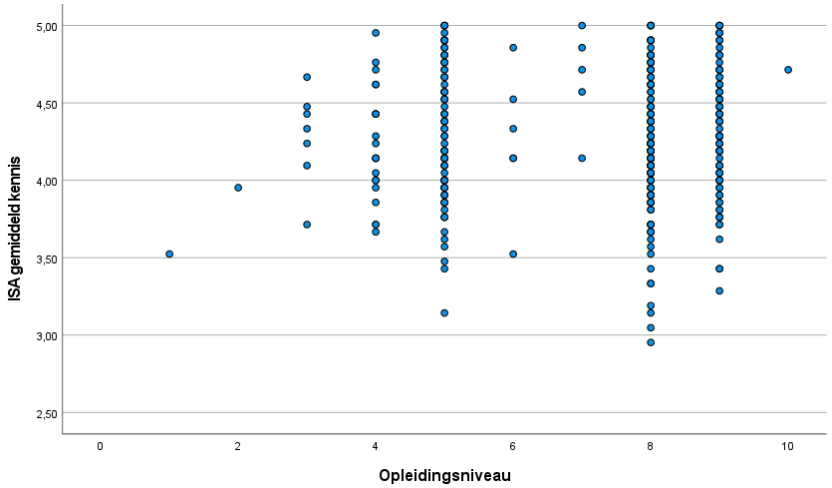


Histogram: frequentie van ISA gemiddeld gedrag

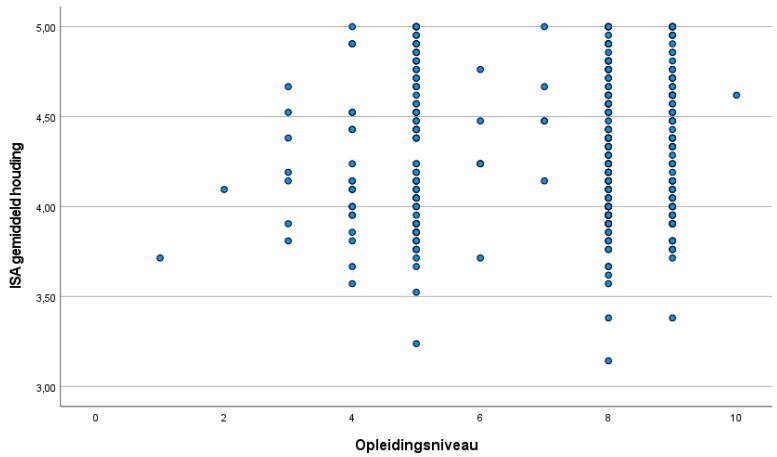
Bijlage 10: Spreidingsdiagrammen opleidingsniveau en ISA totaal, kennis, houding en gedrag



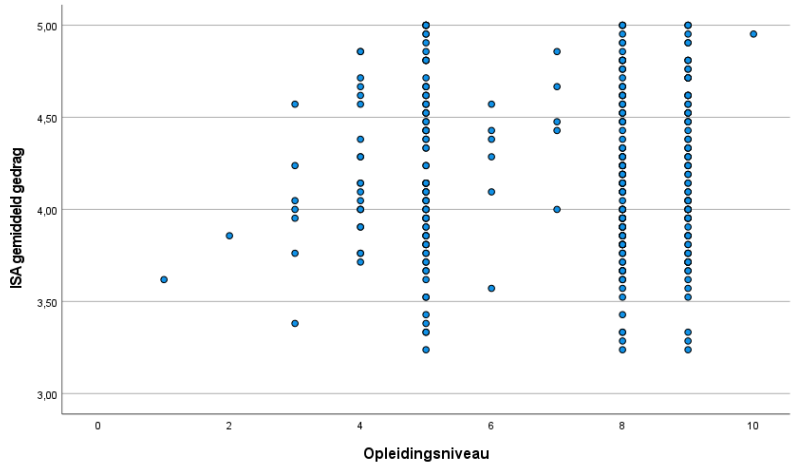
Spreidingsdiagram: ISA gemiddeld totaal



Spreidingsdiagram: ISA gemiddeld kennis



Spreidingsdiagram: ISA gemiddeld houding



Spreidingsdiagram: ISA gemiddeld gedrag

Bijlage 11: Correlatie analyse

Correlations

			ISA gemiddeld totaal	ISA gemiddeld kennis	ISA gemiddeld houding	ISA gemiddeld gedrag	Opleidingsniveau
Spearman's rho	ISA gemiddeld totaal	Correlation Coefficient	1,000	,937**	,941**	,930**	,044
		Sig. (1-tailed)	.	,000	,000	,000	,207
		N	355	355	355	355	355
	ISA gemiddeld kennis	Correlation Coefficient	,937**	1,000	,849**	,798**	,042
		Sig. (1-tailed)	,000	.	,000	,000	,213
		N	355	355	355	355	355
	ISA gemiddeld houding	Correlation Coefficient	,941**	,849**	1,000	,813**	,078
		Sig. (1-tailed)	,000	,000	.	,000	,070
		N	355	355	355	355	355
	ISA gemiddeld gedrag	Correlation Coefficient	,930**	,798**	,813**	1,000	-,003
		Sig. (1-tailed)	,000	,000	,000	.	,475
		N	355	355	355	355	355
	Opleidingsniveau	Correlation Coefficient	,044	,042	,078	-,003	1,000
		Sig. (1-tailed)	,207	,213	,070	,475	.
		N	355	355	355	355	359

**. Correlation is significant at the 0.01 level (1-tailed).

Tabel: Spearman correlatie

Bijlage 12: Variantieanalyse

Report

ISA gemiddeld totaal

Opleidingsniveau	Mean	N	Std. Deviation
Basisonderwijs	3,6190	1	.
VMBO, MBO-niveau 1 entreeopleiding	3,9683	1	.
VMBO, MBO-niveau 2 beroepsopleiding	4,1678	7	,27044
MBO-niveau 3 vakopleiding	4,2192	21	,35992
HAVO, MBO-niveau 4 middenkader- of specialistenopleiding	4,2746	84	,42003
VWO	4,2513	6	,37447
Associate degree	4,5651	5	,27415
Bachelor (HBO of WO)	4,2106	143	,38555
Master (HBO of WO)	4,2911	86	,38096
Doctorsgraad	4,7619	1	.
Total	4,2498	355	,38999

Frequentietabel: ISA gemiddeld totaal

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
ISA gemiddeld totaal * Opleidingsniveau	Between Groups	(Combined)	1,721	9	,191	1,266	,254
	Within Groups		52,120	345	,151		
	Total		53,841	354			

Measures of Association

	Eta	Eta Squared
ISA gemiddeld totaal * Opleidingsniveau	,179	,032

Report

ISA gemiddeld kennis

Opleidingsniveau	Mean	N	Std. Deviation
Basisonderwijs	3,5238	1	.
VMBO, MBO-niveau 1 entreeopleiding	3,9524	1	.
VMBO, MBO-niveau 2 beroepsopleiding	4,2789	7	,30791

MBO-niveau 3 vakopleiding	4,2313	21	,36679
HAVO, MBO-niveau 4 middenkader- of specialistenopleiding	4,2965	84	,43483
VWO	4,2540	6	,44738
Associate degree	4,6571	5	,32888
Bachelor (HBO of WO)	4,2221	143	,42704
Master (HBO of WO)	4,3189	86	,40466
Doctorsgraad	4,7143	1	.
Total	4,2702	355	,41995

Frequentietabel: ISA gemiddeld kennis

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
ISA gemiddeld kennis * Opleidingsniveau	Between Groups	(Combined)	2,231	9	,248	1,421	,178
	Within Groups		60,200	345	,174		
	Total		62,431	354			

Measures of Association

	Eta	Eta Squared
ISA gemiddeld kennis * Opleidingsniveau	,189	,036

Report

ISA gemiddeld houding

Opleidingsniveau	Mean	N	Std. Deviation
Basisonderwijs	3,7143	1	.
VMBO, MBO-niveau 1 entreeopleiding	4,0952	1	.
VMBO, MBO-niveau 2 beroepsopleiding	4,2313	7	,31398
MBO-niveau 3 vakopleiding	4,2018	21	,39810
HAVO, MBO-niveau 4 middenkader- of specialistenopleiding	4,3067	84	,43351
VWO	4,2778	6	,34525
Associate degree	4,5524	5	,31335
Bachelor (HBO of WO)	4,2617	143	,38690
Master (HBO of WO)	4,3594	86	,40132
Doctorsgraad	4,6190	1	.
Total	4,2952	355	,40072

Frequentietabel: ISA gemiddeld houding

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
ISA gemiddeld houding * Opleidingsniveau	Between Groups	(Combined)	1,552	9	,172	1,076	,380
	Within Groups		55,294	345	,160		
	Total		56,845	354			

Measures of Association

	Eta	Eta Squared
ISA gemiddeld houding * Opleidingsniveau	,165	,027

Report

ISA gemiddeld gedrag

Opleidingsniveau	Mean	N	Std. Deviation
Basisonderwijs	3,6190	1	.
VMBO, MBO-niveau 1 entreeopleiding	3,8571	1	.
VMBO, MBO-niveau 2 beroepsopleiding	3,9932	7	,37134
MBO-niveau 3 vakopleiding	4,2245	21	,36395
HAVO, MBO-niveau 4 middenkader- of specialistenopleiding	4,2205	84	,46831
VWO	4,2222	6	,35592
Associate degree	4,4857	5	,32015
Bachelor (HBO of WO)	4,1479	143	,40826
Master (HBO of WO)	4,1949	86	,43279
Doctorsgraad	4,9524	1	.
Total	4,1839	355	,42649

Frequentietabel: ISA gemiddeld gedrag

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
ISA gemiddeld gedrag * Opleidingsniveau	Between Groups	(Combined)	2,079	9	,231	1,279	,247
	Within Groups		62,312	345	,181		
	Total		64,391	354			

Measures of Association

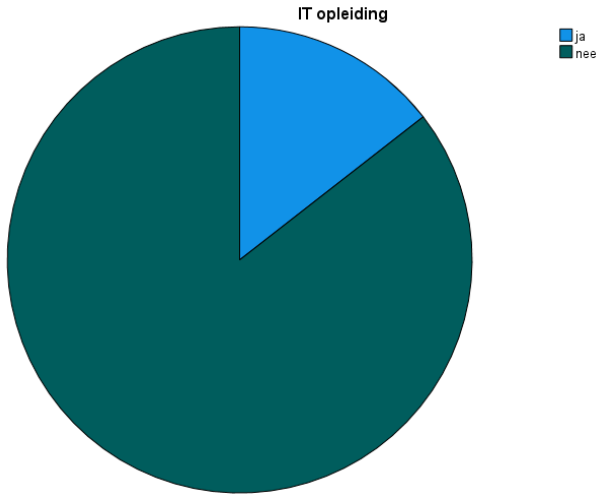
	Eta	Eta Squared
ISA gemiddeld gedrag * Opleidingsniveau	,180	,032

Bijlage 13: T-toets

IT-opleiding

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ja	52	14,5	14,5	14,5
	nee	307	85,5	85,5	100,0
	Total	359	100,0	100,0	

Frequentietabel: IT-opleiding ja/nee



Cirkeldiagram: IT-opleiding ja/nee

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
ISA gemiddeld totaal	Equal variances assumed	3,087	0,080	4,694	353	0,000
	Equal variances not assumed			5,424	77,581	0,000

T-toets: ISA totaal.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
ISA gemiddeld kennis	Equal variances assumed	4,093	0,044	4,449	353	0,000
	Equal variances not assumed			5,486	83,781	0,000

T-toets: ISA kennis.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
ISA gemiddeld houding	Equal variances assumed	3,156	0,077	4,268	353	0,000
	Equal variances not assumed			4,734	74,343	0,000

T-toets: ISA houding.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
ISA gemiddeld gedrag	Equal variances assumed	1,049	0,306	4,439	353	0,000
	Equal variances not assumed			4,924	74,363	0,000

T-toets: ISA gedrag.